ĐẠI HỌC KHOA HỌC TỰ NHIÊN TP. HỒ CHÍ MINH

KHOA ĐIỆN TỬ - VIỄN THÔNG

BỘ MÔN VIỄN THÔNG VÀ MẠNG

------oOo------

BÁO CÁO ĐỀ TÀI:

IPSEC over TCP/UDP

GVHD: Trần Thị Thảo Nguyên

Nhóm trình bày :

Hoàng Đức Phú	0920090
Nguyễn Hùng Cường	0920010
Hồ Minh Tâm	0920219
Nguyễn Thanh Hùng	0920181
Phan Thị Xuân Lan	0920054

Nhóm phản biện :

Nguyễn Hoài Nhân	0920078
Đặng Ngàn Nhất Phương	0920092
Trần Thị Như Thắm	0920223
Võ Quốc Anh	0920149

MỤC LỤC

I. GIỚI THIỆU :

1. Nhu cầu sử dụng IP Sec hiện nay:

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) là một giao thức được chuẩn hoá bởi IETF 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 IPSec cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI.

IPSec được thiết kế như phần mở rộng của giao thức IP, được thực hiện thống nhất trong cả hai phiên bản IPv4 và IPv6. Đối với IPv4, việc áp dụng IPSec là một tuỳ chọn, nhưng đối với IPv6, giao thức bảo mật này được triển khai bắt buộc.

2. Khái niệm IP Sec :

IPSec (Internet Protocol Security) là một giao thức được IETF phát triển. IPSec được định nghĩa là một giao thức trong tầng mạng cung cấp các dịch vụ bảo mật, nhận thực, toàn vẹn dữ liệu và điều khiển truy cập. Nó là một tập

hợp các tiêu chuẩn mở làm việc cùng nhau giữa các phần thiết bị.

Một cách chung nhất, IPSec cho phép một đường ngầm bảo mật thiết lập giữa 2 mạng riêng và nhận thực hai đầu của đường ngầm này. Các thiết bị giữa hai đầu đường ngầm có thể là một cặp host, hoặc một cặp cổng bảo mật (có thể là router, firewall, bộ tập trung VPN) hoặc một cặp thiết bị gồm một host và một cổng bảo mật. Đường ngầm đóng vai trò là một kênh truyền bảo mật giữa hai đầu và các gói dữ liệu yêu cầu an toàn được truyền trên đó. IPSec cũng thực hiện đóng gói dữ liệu các thông tin để thiết lập, duy trì và hủy bỏ kênh truyền khi không dùng đến nữa. Các gói tin truyền trong đường ngầm có khuôn dạng giống như các gói tin bình thường khác và không làm thay đổi các thiết bị, kiến trúc cũng như những ứng dụng hiện có trên mạng trung gian, qua đó cho phép giảm đáng kể chi phí để triển khai và quản lý.

IPSec có các cơ chế cơ bản để đảm bảo an toàn dữ liệu đó là AH (Authentication Header), ESP (Encapsulating Security Payload), IKE (Internet Key Exchange) và ISAKMP (Internet Security Association and Key Management Protocol) trong đó IPSec phải hỗ trợ ESP và có thể hỗ trợ AH:

- AH cho phép xác thực nguồn gốc dữ liệu, kiểm tra tính toàn vẹn dữ liệu và dịch vụ tùy chọn chống phát lại của các gói IP truyền giữa hai hệ thống. AH không cung cấp tính bảo mật, điều này có nghĩa là nó gửi đi thông tin dưới dạng bản rõ.
- ESP là một giao thức cung cấp tính an toàn của các gói tin được truyền bao gồm: Mật mã dữ liệu, xác thực nguồn gốc dữ liệu, kiểm tra tính toàn vẹn phi kết nối của dữ liệu. ESP đảm bảo tính bí mật của thông tin thông qua việc mật mã gói tin IP. Tất cả lưu lương ESP đều được mật mã giữa hai hệ thống. Với đặc điểm này thì xu hướng sẽ sử dụng ESP nhiều hơn AH để tăng tính an toàn cho dữ liệu.
- Cả AH và ESP là các phương tiện cho điều khiển truy nhập, dựa vào sự phân phối của các khóa mật mã và quản lý các luồng giao thông có liên quan đến những giao thức an toàn này.

- IKE (Internet Key Exchange): IKE là giao thức thực hiện quá trình trao đổi khóa và thỏa thuận các thông số bảo mật giữa các thiết bị với nhau như: mã hóa thế nào, dùng thuật toán nào, bao lâu trao đổi khóa một lần. Sau khi trao đổi xong thì sẽ có một thương lượng giữa hai đầu cuối, khi đó IPsec SA (Security Association) được tạo ra. Một SA, là một liên kết bảo mật, có thể được xem là một nhóm những thành phần, thông số bảo mật đã được thống nhất giữa 2 đầu cuối, nói cách khác, khi tất cả các thông số đã được thương lượng và các khóa đã được tạo ra, một thiết bị có 1 SA và nó có thể sử dụng SA này để giao tiếp với một thiết bị khác.

- ISAKMP (Internet Security Association and Key Management Protocol): là một giao thức thực hiện việc thiết lập, thỏa thuận và quản lý chính sách bảo mật SA. Giao thức này đi kèm với giao thức IKE nên ta sẽ viết ISAKMP/IKE.

Những giao thức này có thể được áp dụng một mình hay kết hợp với nhau để cung cấp tập các giao thức an toàn mong muốn trong IPv4 và IPv6, nhưng cách chúng cung cấp các dịch vụ là khác nhau. Đối với cả hai giao thức AH và ESP này, IPSec không định các thuật toán an toàn cụ thể được sử dụng, mà thay vào đó là một khung chuẩn để sử dụng các thuật toán theo tiêu chuẩn công nghiệp. IPSec sử dụng các thuật toán: Mã nhận thực bản tin trên cơ sở băm (HMAC), thuật toán MD5 (Message Digest 5), thuật toán SHA-1 để thực hiện chức năng toàn vẹn bản tin; Thuật toán DES, 3DES để mật mã dữ liệu; Thuật toán khóa chia sẻ trước, RSA chữ ký số và RSA mật mã giá trị ngẫu nhiên (Nonces) để nhận thực các bên. Ngoài ra các chuẩn còn định nghĩa việc sử dụng các thuật toán khác như IDEA, Blowfish và RC4. IPSec có thể sử dụng giao thức IKE (Internet Key Exchange) để xác thực hai phía và làm giao thức thương lượng các chính sách bảo mật và nhận thực thông qua việc xác định thuật toán được dùng để thiết lập kênh truyền, trao đổi khóa cho mỗi phiên kết nối, dùng trong mỗi phiên truy cập. Mạng dùng IPSec để bảo mật các dòng dữ liệu có thể tự động kiểm tra tính xác thực của thiết bị bằng giấy chứng nhận số của hai người dùng trao đổi thông tin qua

lại. Việc thương lượng này cuối cùng dẫn đến thiết lập kết hợp an ninh (SAS) giữa các cặp bảo mật, kết hợp an ninh này có tính chất hai chiều trực tiếp. Thông tin kết hợp an ninh được lưu trong cơ sử dữ liệu liên kế an ninh, và mỗi SA được ấn định một số tham số an ninh trong bảng mục lục sao cho khi kết hợp một địa chỉ đích với giao thức an ninh (ESP hoặc AH) thì có duy nhất một.

3. Lịch sử phát triển của IP Sec:

Từ khi công nghệ ipsec ra đời, nó không chỉ còn được biết đến như một chuẩn interrnet đơn lẽ nữa, mà hơn thế nữa còn được định nghĩa trong chuẩn RFC, được kể đến trong bảng sau:

RFC	**Tiêu đề**	**Chủ đề**	**Thời gian**
1825	Security Architure for the Internet Protocol (kiến trúc bảo mật cho giao thức Internet)	IPSec	8/1995
1826	IP Authentication Header (Nhận thực tiêu đề IP)	AH	8/1995
1827	IP Encapsulating Security Payload (đóng gói an toàn tải IP)	ESP	8/1995
1828	IP Authentication Using Keyed MD5 (Nhận thực IP sử dụng khoá MD5)	MD5	8/1995
1829	The ESP DES-CBC Transform (sự biến đổi ESP nhờ DES-CBC)	DES	8/1995
2104	HMAC: Keyed-Hashing for Message Authentication (HMAC: Khoá băm cho nhận thực bản	HMAC	1/1997

	tin)		
2202	Test Cases for HMAC-MD5 and HMAC-SHA-1 (các trường hợp kiểm tra cho HMAC-MD5 và HMAC-SHA-1)	HMAC-MD5 HMAC-SHA-1	9/1997
2401	Security Architure for Internet Protocol	IPSec	10/1998
2402	IP Authentication Header	AH	10/1998
2403	The Use of HMAC-MD5-96 within ESP and AH (sử dụng HMAC-MD5-96 cùng với ESP)	HMAC-MD5	10/1998
2404	The Use of HMAC-SHA-1-96 within ESP and AH (sử dụng HMAC-SHA-1-96 cùng với ESP và AH)	HMAC-SHA-1	10/1998
2405	The ESP DES-CBC Cipher Algorithm With Explicit IV (Thuật toán mã hoá ESP DES-CBC cùng IV (vector khởi tạo))	DES	10/1998
2406	IP Encapsulating Security Payload	ESP	10/1998
2407	The Internet IP Security Domain of Interpretation for ISAKMP (bảo mật gói tin IP trong phạm vi làm sáng tỏ ISAKMP)	ISAKMP	10/1998
2408	Internet Security Association and Key Management Protocol (giao thức quản lý kết hợp an ninh	ISAKMP	10/1998

	Internet và Khoá)		
2409	The Internet Key Exchange (phương thức trao đổi khoá internet)	IKE	10/1998
2410	The NULL Encryption Algorithm and Its Use With IPSec (vô hiệu thuật toán bảo mật và sử dụng nó với IPSec)	NULL	10/1998
2451	The ESP CBC-Mode Cipher Algorithms (thuật toán mật mã kiểu CBC cho ESP)	CBC	10/1998

II. KẾT NỐI IP SEC:

Phần này sẽ trình bày về quá trình tạo kết nối để chia sẻ dữ liệu một cách bảo mật giữa hai thiết bị IPsec. Hai thiết bị đó phải đi qua 5 bước cơ bản sau đây:

1. Kết nối IPsec sẽ được bắt đầu nếu có một yêu cầu nào đó, thường là yêu cầu cần có 1 kết nối bảo mật từ một thiết bị muốn kết nối với một thiết bị đích. Tất nhiên người quản trị hoặc một người dùng bất kỳ đều có thể bắt đầu quá trình này từ thiết bị của họ.
2. Nếu chưa có một kết nối VPN nào tồn tại, IPsec sẽ sử dụng ISAKMP/IKE Phase 1 để tạo một *kết nối quản lý* bảo mật. Kết nối quản lý này là cần thiết vì nó đảm bảo cho 2 thiết bị có thể liên lạc với nhau một cách an toàn, hơn nữa, nó có thể từ đó xây dựng một kết nối dữ liệu bảo mật.
3. Thông qua kết nối quản lý bảo mật này, hai thiết bị sẽ thương lượng, thống nhất các thông số bảo mật được sử dụng để tạo nên một *kết nối dữ liệu*. Các kết nối dữ liệu được dùng để truyền các dữ liệu như files, Telnets, email, video, voice,…

4. Khi kết nối dữ liệu đã được tạo, các thiết bị IPsec có thể sử dụng nó để truyền dữ liệu một cách an toàn. Nếu hàm HMAC được sử dụng ở thiết bị nguồn để tạo ra chữ ký số, thì thiết bị đích sẽ kiểm tra các chữ ký này để xác định tính toàn vẹn của dữ liệu cũng như chứng thực thông tin đó là đúng hay sai. Ngoài ra, nếu dữ liệu được mã hóa tại nguồn thì tại đích nó sẽ được giải mã.
5. Cả kết nối quản lý và kết nối dữ liệu đều có một thời gian tồn tại (lifetime) xác định. Điều này là để đảm bảo cho các khóa bảo mật sẽ được tạo lại và khác với lúc trước, do đó tránh được trường hợp ai đó sẽ tìm cách phá khóa bảo mật của bạn. Khi hết thời hạn lifetime này, kết nối sẽ tự động đóng lại và được tạo lại nếu ta tiếp tục cần gửi dữ liệu.

Để có cái nhìn cụ thể hơn về giao thức IPsec. Các phần sau đây sẽ lần lượt trình bày về các giai đoạn (Phase) hoạt động của ISAKMP/IKE.

III. ISAKMP/IKE GIAI ĐOẠN 1: TẠO KẾT NỐI QUẢN LÝ:

Trong phần này chúng ta sẽ làm rõ hơn các bước để thiết lập một kết nối quản lý IPsec.

ISAKMP và IKE hoạt động cùng nhau để thiết lập một kết nối bảo mật, an toàn hơn giữa hai thiết bị. ISAKMP định nghĩa các thông số của gói tin, với cơ chế là một giao thức trao đổi khóa (Key), và thực hiện một quá trình đàm phán. Tuy nhiên giao thức ISAKMP không định nghĩa cách tạo, chia sẻ Key, hoặc quản lý kết nối bảo mật như thế nào mà giao thức IKE sẽ thực hiện việc này.

Để hiểu rõ chi tiết ISAKMP/IKE thiết lập một kết nối quản lý như thế nào? Phần sau đây sẽ bao gồm các ý sau:

+ Kết nối quản lý.
+ Giao thức trao đổi Key: Diffie-Hellman.
+ Chứng thực thiết bị.

A. Kết nối quản lý:

Kết nối được thiết lập trong giai đoạn 1. Kết nối này sử dụng giao tiếp UDP port 500. Đây là một kết nối 2 chiều, 2 peers có thể chia sẻ các thông điệp IPsec cho nhau.

Lưu ý: Các kết nối ISAKMP/IKE sử dụng giao thức UDP. Port nguồn và đích là 500; tuy nhiên, một vài nhà cung cấp sử dụng số port ngẫu nhiên lớn hơn 1023 thay vì 500.

Dù là một kết nối site-to-site hay là kết nối từ xa, có 3 điều sau đây sẽ xảy ra trong quá trình ISAKMP/IKE giai đoạn 1:

1. Các peers sẽ đàm phán với nhau về việc kết nối quản lý sẽ được bảo vệ như thế nào.
2. Các peers sẽ dùng thuật toán Diffie-Hellman để chia sẻ thông tin về Key để bảo vệ việc quản lý kết nối.
3. Các peers sẽ định danh, xác nhận với nhau trước khi quá trình ISAKMP/IKE giai đoạn 2 diễn ra.

ISAKMP/IKE giai đoạn 1 chịu trách nhiệm cho việc thiết lập kết nối quản lý an toàn. Tuy nhiên ta lại có 2 chế độ để thực hiện 3 bước trên:

+ Main (chế độ chính).

+ Aggressive (chế độ linh hoạt).

1. Main Mode:

Main mode thực hiện 3 trao đổi 2 chiều, tổng cộng là 6 packets. Ba sự trao đổi là 3 bước được liệt kê trong phần trên: đàm phán chính sách bảo mật sử dụng để quản lý kết nối, sử dụng Diffie-Hellman để mã hóa keys dùng cho thuật toán mã hóa và hàm HMAC đã được đàm phán ở bước 1, và thực hiện xác thực thiết bị sử dụng một trong ba cách sau: pre-shared keys, RSA encrypted nonces (khóa RSA sử dụng một lần) hoặc RSA signatures (digital certificates – chứng thực số).

Main mode có một ưu điểm: bước xác thực thiết bị diễn ra thông suốt trong cả quá trình kết nối quản lý, vì kết nối này đã được xây dựng ở hai bước

đầu tiên trước khi việc chứng thực thiết bị diễn ra. Nên bất kì thông tin nhận dạng của 2 peers gởi cho nhau đều được bảo vệ khỏi các cuộc nghe trộm.

Main Mode là mode mặc định của Cisco cho kết nối site-to-site và kết nối từ xa.

2. Aggressive Mode:

Trong mode này, chỉ có 2 quá trình trao đổi. Trao đổi đầu tiên bao gồm danh sách các chính sách bảo mật sử dụng cho kết nối quản lý, public key có được từ cặp "public/private key" được tạo ra bởi DH, các thông tin nhận dạng, thông tin xác minh các thông tin nhận dạng (ví dụ như chữ ký). Tất cả đều được ép vào một gói tin. Quá trình trao đổi thứ 2 là sự trả lời (ACK) cho gói vừa nhận được, ngoài ra nó còn chia sẻ key đã mã hóa (dùng thuật toán DH), và thông tin kết nối quản lý đã được thiết lập thành công hay chưa.

Aggressive Mode có một ưu điểm hơn Main Mode: kết nối quản lý được thiết lập nhanh hơn, tuy nhiên nhược điểm của nó là bất kì những thông tin nhận dạng được gởi đều là clear text. Do đó, nếu một ai đó nghe trộm thông tin trên đường truyền, họ có thể biết được các thông tin nhận dạng sử dụng để tạo chữ ký cho việc xác thực thiết bị. Vì vậy, nếu ta lo lắng về việc có thể bị xem trộm thông tin nhận dạng thiết bị, ta nên sử dụng Main Mode.

3. ISAKMP/IKE Transforms:

Một trong những điều đầu tiên 2 peers phải thực hiện trong quá trình ISAKMP/IKE giai đoạn 1 là việc đàm phán xem kết nối quản lý sẽ được bảo vệ như thế nào. Điều này được thực hiện bằng cách xác định **transforms** (các biến đổi). Một transform là một danh sách các biện pháp an ninh nên được sử dụng để bảo vệ kết nối. Với riêng ISAKMP/IKE giai đoạn 1, Transform đôi khi được gọi là một chính sách IKE hay ISAKMP.

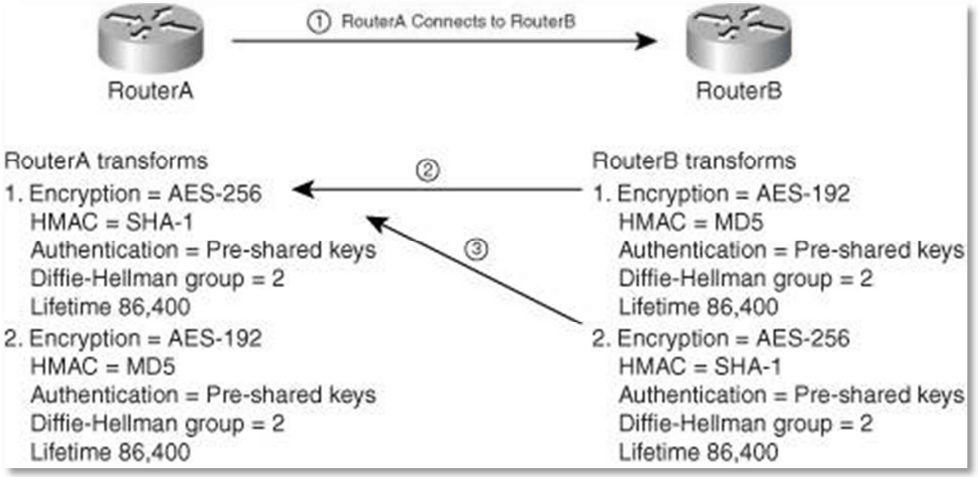
Các thông tin bao gồm trong một Transform Giai đoạn 1 là:

- Thuật toán mã hóa: DES, 3DES hoặc AES.
- Các hàm HMAC sử dụng: MD5 hay SHA-1.
- Kiểu xác thực thiết bị: pre-shared keys, RSA encrypted nonces, or RSA signatures (certificates).

- Nhóm khóa Diffie-Hellman: Cisco chỉ cung cấp 1, 2, 5, 7. Với 7 thì chỉ cung cấp trên Cisco 3000 concentrators và PIX và ASA những ứng dụng bảo mật đang chạy phiên bản 7.0.
- Thời gian tồn tại của một kết nối quản lý.

Tổng hợp lại, tất cả những mục này được coi như là một bộ biến đổi (transform set). Thiết bị IPsec của bạn có thể cần nhiều bộ transform khác nhau. Ví dụ như nếu thiết bị của bạn cần kết nối IPsec đến 2 peers, mỗi peer lại có một kiểu mã hóa khác nhau, như DES hay 3DES. Thì ta phải cần những transform khác nhau để tận dụng lợi thế vừa dùng 3DES đến một peer này và DES đến một peer khác.

Thiết bị của bạn cần phải gởi toàn bộ danh sách ISAKMP/IKE transforms đến remote peer. Thứ tự trong transform được gởi đi rất quan trọng vì những cái nào khớp với remote peer trước sẽ được sử dụng ngay. Ví dụ, thiết bị của bạn khởi tạo kết nối đến remote peer và gởi đến 1 danh sách transform cho thiết bị từ xa đó. Remote peer sẽ so sánh với danh sách của nó để tìm những transform nào khớp với nó. Thiết bị bắt đầu dò từ cái đầu tiên trong danh sách bạn gởi so với cái đầu trong danh sách của nó. Nếu trùng thì transform đó được sử dụng ngay. Nếu không, nó tiếp tục so sánh với cái thứ 2 trong danh sách… Trường hợp khi so sánh cái đầu tiên của bạn với toàn bộ danh sách của nó mà không có sự trùng khớp nào, thiết bị từ xa đó sẽ tiếp tục so sánh transform thứ hai của bạn với toàn bộ tranform của thiết bị đó.



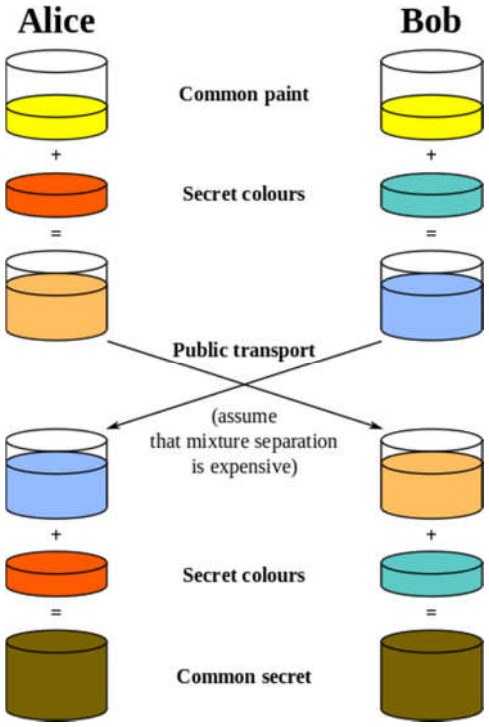
Ví dụ về quá trình diễn ra sự thương lượng (Nguồn: The Complete Cisco VPN Configuration Guide – Richard Deal)

Lưu ý: nếu quá trình này không tìm thấy sự khớp nhau nào giữa 2 peers thì kết nối quản lý sẽ không được thiết lập và IPsec sẽ thất bại. Có một ngoại lệ là thông số thời gian tồn tại của mỗi peer không cần khớp với nhau, nếu không khớp thì chúng sẽ lấy giá trị nào nhỏ hơn. Tuy nhiên, một số nhà cung cấp không tuân theo mặc định của IPsec, khi đó bạn phải làm khớp 2 giá trị thời gian sống trên 2 peers.

B. Giao thức trao đổi key: Diffie-Hellman (DH):

Một khi các peers đã đàm phán các chính sách bảo vệ sử dụng cho kết nối quản lý trong Giai đoạn 1, DH được dùng để tạo một khóa bí mật (secret key). Hai giao thức ISAKMP và IKE không dùng để chia sẻ dữ liệu tạo key trên một mạng không an toàn, mà thay vào đó chính DH sẽ thực hiện nhiệm vụ này.

Ta định nghĩa sơ lược về DH như sau: cả 2 peers đều tạo ta một kết hợp "public/private key", public. Chúng chia sẻ public key với nhau. Chúng giữ lại private key và nhận public key từ remote access, từ hai key này thông qua một hàm tính toán, sẽ tạo ra một secret key, secret key này ở cả 2 peers sẽ giống nhau và nó được sử dụng để mã hóa bất cứ những thông tin quan trọng nào. Nếu người ở giữa muốn nghe trộm thông tin thì phải có một trong hai private key của 1 trong 2 peers thì mới có thể tính ra secret key, nhưng tất nhiên, private key thì không được chia sẻ với ai cả!



Ví dụ về việc trao đổi khóa DH (hàng thứ 2 và 5 xem như private key, hàng thứ 3 xem như public key, hàng thứ 4 là các public key sau khi trao đổi với nhau, hàng cuối cùng chính là secret key) (Nguồn: wikipedia)

Nhóm DH key là những nhóm dùng độ dài khác nhau để mã hóa key. Có nhiều nhóm DH key được sử dụng, Cisco cung cấp ba nhóm sau:

Nhóm 1: 768 bit

Nhóm 2: 1024 bit

Nhóm 5: 1536 bit

Ngoài ra Cisco còn cung cấp nhóm 7 cho một vài thiết bị khác.

C. Chứng thực thiết bị:

Một vấn đề khi thực hiện với DH là khi bạn muốn trao đổi khóa nhưng lại không biết trước số lượng remote peers. Do đó, trước khi có bất kì một kết nối nào xảy ra, bạn phải xác thực danh tính của remote peer. Với Aggressive Mode trong giai đoạn 1, việc đàm phán, DH, và kiểm tra xác thực diễn ra trong 1 bước lớn duy nhất. Tuy nhiên với Main Mode, quá trình thiết lập cần 3 bước, trong bước 3 việc xác thực dịch vụ lúc này mới được diễn ra, việc xác thực hoàn toàn được thực hiện dưới một kết nối an toàn đã được thiết lập trong bước

1 và 2. Do đó, ưu điểm là bất kì thông tin trao đổi giữa 2 peers đều được thực hiện trong một kết nối đã được bảo vệ.

Trong cả hai chế độ mode, việc xác thực danh tính là phần quan trọng trong IPsec. Có 3 phương pháp cơ bản thực hiện việc này:

1. Symmetric pre-shared keys (thường được gọi ngắn gọn là preshared-key).
2. Asymmetric pre-shared keys (thường gọi là mã hóa RSA một lần).
3. Digital certificates (thường được gọi là chữ ký RSA).

Hai peers sẽ đàm phán với nhau qua transform của quá trình ISAKMP/IKE giai đoạn 1 để thống nhất sẽ sử dụng phương pháp nào. Không phải mọi thiết bị đều hỗ trợ cả 3 phương pháp này. Ví dụ, khi nhìn vào các dòng sản phẩm của Cisco, thì Cisco IOS Router hỗ trợ cả ba. Các sản phẩm khác của Cisco chỉ hỗ trợ hai: pre-shared symmetric keys và digital certificates.

IV. ISAKMP/IKE GIAI ĐOẠN 2: TẠO KẾT NỐI DỮ LIỆU:

Phần này chúng ta sẽ thảo luận làm thế nào để bảo vệ các kết nối dữ liệu người dùng dựa vào những điều sau đây:

- Những thành phần trong ISAKMP/IKE giai đoạn 2.
- Các giao thức bảo mật trong ISAKMP/IKE giai đoạn 2.
- Các phương thức kết nối trong ISAKMP/IKE giai đoạn 2.
- Transforms.
- Kết nối dữ liệu.

A. <u>Những thành phần trong ISAKMP/IKE giai đoạn 2:</u>

ISAKPM/IKE giai đoạn 2 chỉ có một mode được gọi là Quick mode. Quick mode định nghĩa việc bảo vệ các kết nối dữ liệu được xây dựng giữa hai IPsec peers. Quick mode có 2 chức năng chính:

- Thương lượng các thông số bảo mật để bảo vệ các kết nối dữ liệu.
- Luôn đổi mới các thông tin một cách định kỳ (tức là xây dựng lại kết nối).

ISAKMP/IKE giai đoạn 2 có một đặc tính đặc biệt: có 2 luồng kết nối dữ liệu đơn hướng được xây dựng giữa hai thiết bị ngang hàng. Ví dụ, thiết bị A sẽ có một kết nối dữ liệu đến thiết bị B và thiết bị B sẽ có một kết nối dữ liệu riêng để đến thiết bị A. Do 2 kết nối này là tách biệt với nhau, nên các thông số bảo mật được đàm phán có thể khác nhau giữa 2 thiết bị này. Ví dụ như kết nối A-B có thể sử dụng 3DES cho việc mã hóa, nhưng kết nối B-A có thể sử dụng DES. Tuy nhiên, điều này thường không được áp dụng vì các thông số bảo mật luôn tương tự nhau.

Sau đây là các chính sách cần xác định để cấu hình các thiết bị nhằm xây dựng các kết nối ISAKMP/IKE giai đoạn 2 phù hợp với yêu cầu:

- Luồng dữ liệu nào mới thực sự cần được bảo vệ?
- Cần sử dụng giao thức bảo mật nào? AH hay ESP.
- Dựa vào việc lựa chọn các giao thức bảo mật, các luồng dữ liệu sẽ được bảo vệ bằng cách nào? Dùng hàm băm hay hàm mã hóa.
- Dùng tunnel hay transport mode?
- Khi xây dựng lại kết nối, ISAKMP/IKE giai đoạn 1 có nên tạo lại và chia sẻ các khóa mới hay không thay vì giữ nguyên khóa cũ.
- Thời gian sống của các kết nối dữ liệu là bao nhiêu?

B. <u>Các giao thức bảo mật giai đoạn 2:</u>

IPsec có thể sử dụng một hay hai giao thức bảo mật sau đây để bảo vệ dữ liệu được truyền qua các kết nối dữ liệu được xây dựng trong ISAKMP/IKE giai đoạn 2:

- AH
- ESP

Bảng dưới đây so sánh 2 giao thức này.

Đặc điểm bảo mật	AH	ESP
Số hiệu giao thức lớp 3	51	50
Hỗ trợ tính toàn vẹn dữ liệu	Yes	Yes
Hỗ trợ chứng thực dữ liệu	Yes	Yes
Hỗ trợ mã hóa dữ liệu	No	Yes

Bảo vệ dữ liệu trước tấn công replay	Yes	Yes
Hoạt động với NAT	No	Yes
Hoạt động với PAT	No	No
Bảo vệ cho gói tin IP	Yes	No
Chỉ bảo vệ cho dữ liệu	No	Yes

1. Giao thức Authentication Header (AH):

1.1 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).

1.2 Cấu trúc gói AH:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

- *Ý nghĩa từng phần:*
  - Next Header (tiêu đề tiếp theo) Có độ dài 8 bit 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 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 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 2^{32} 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.

1.3 Quá trình xử lý AH:

Hoạt động của AH được thực hiện qua các bước như sau:

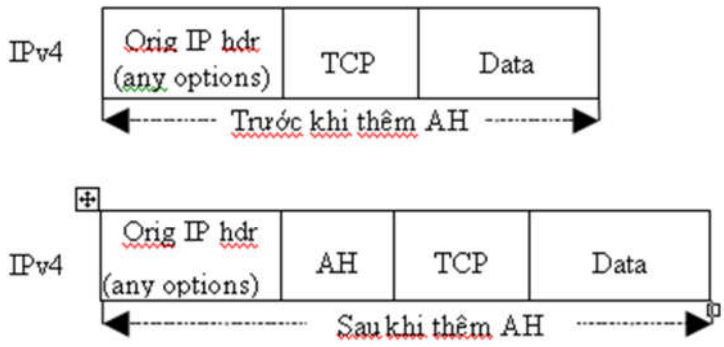
- Bước 1: Toàn bộ gói IP (bao gồm IP header và tải tin) được thực hiện qua một hàm băm một chiều.
- Bước 2: Mã hash thu được dùng để xây dựng một AH header, đưa header này vào gói dữ liệu ban đầu.

- Bước 3: Gói dữ liệu sau khi thêm AH header được truyền tới đối tác IPSec.
- Bước 4: Bên thu thực hiện hàm băm với IP header và tải tin, kết quả thu được một mã hash.
- Bước 5: Bên thu tách mã hash trong AH header.
- Bước 6: 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.

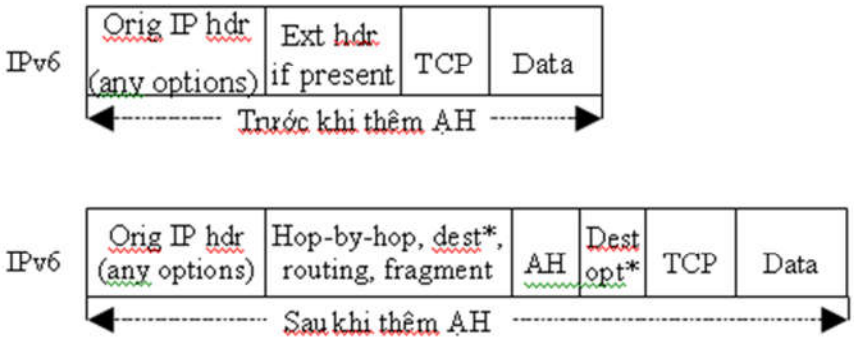
a. Vị trí của Header:

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.

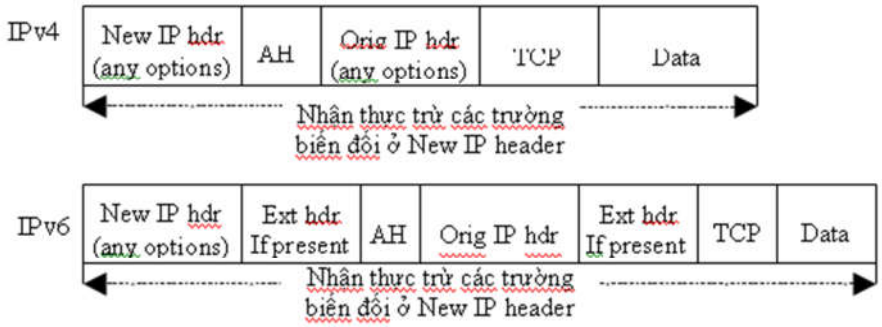


Khuôn dạng IPv4 trước và sau khi xử lý AH ở kiểu Transport



Khuôn dạng IPv6 trước và sau khi xử lý AH ở kiểu Traport

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.



Khuôn dạng gói tin đã xử lý AH ở kiểu Tunnel

b. *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.

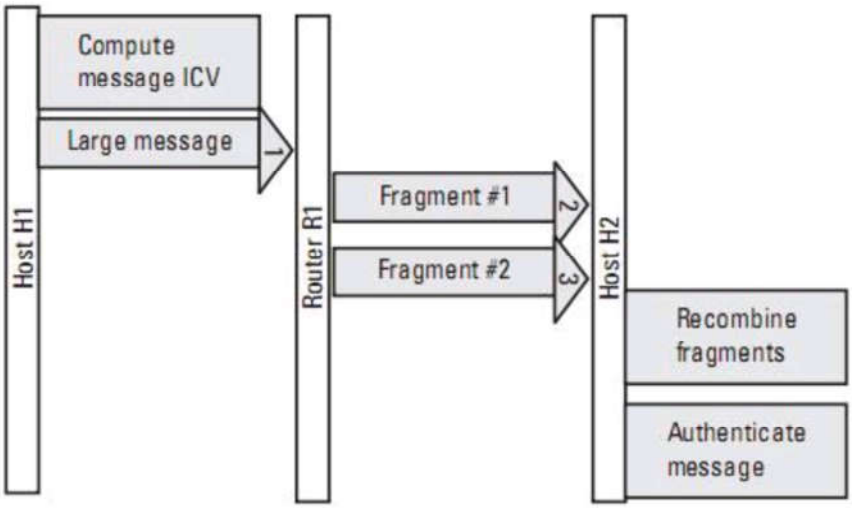
c. *Xử lý gói đầu ra:*

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:

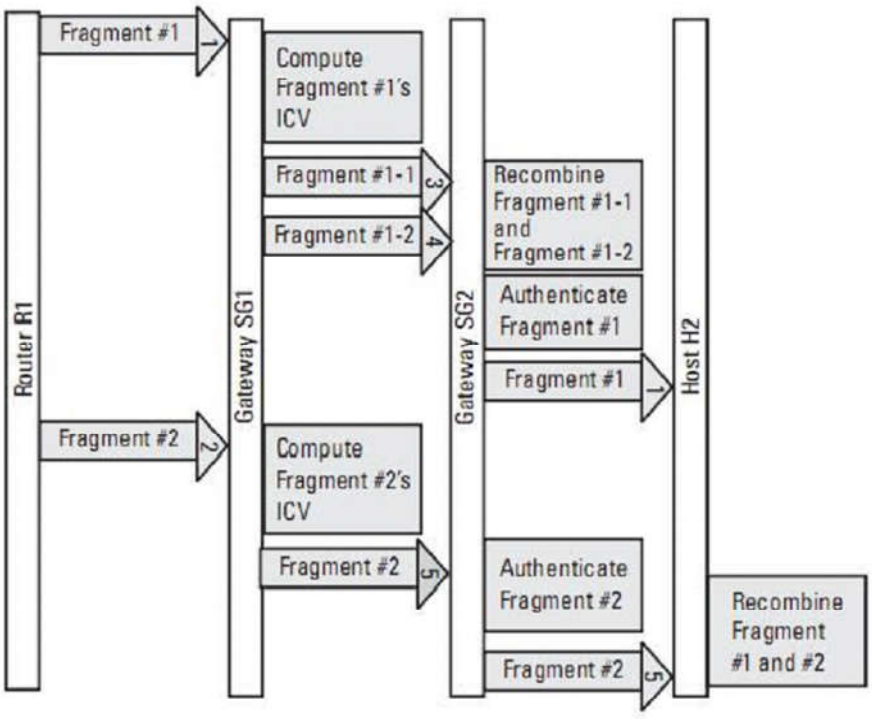
- Tìm kiếm SA: AH được thực hiện trên gói tin đầu ra chỉ khi quá trình IPSec đã xác định được gói tin đó được liên kết với một SA. SA đó sẽ yêu cầu AH xử lý gói tin. Việc xác định quá trình xử lý IPSec nào cần thực hiện trên lưu lượng đầu ra có thể xem trong RFC 2401
- Tạo SN: bộ đếm phía phát được khởi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



Fragmentation and authentication: Transport Mode host-to-host SA.



Fragmentation and authentication: Tunnel Mode gateway-to-gateway SA.

d. <u>Xử lý gói đầu vào:</u>

Khi nhận được một thông điệp có chứa AH, quá trình xử lí ip trước tiên sẽ tổng 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 mode nào 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 sang tunnel 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 điệp nào có sequence number nhỏ hơn miền giá trị của cửa sổ phát lại đều 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 sử 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 cửa 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

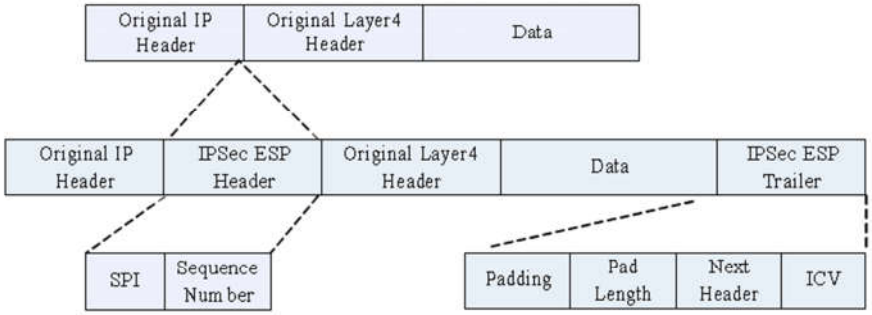
cận đến các protocol của lớp trên gói tin được gửi đến chu trình xử lí gói ip tiếp tục di chuyển trong tầng ip. Trong trường hợp khác, nếu quá trình xử lí tiếp cận với một tunnel ip header mà đích đến không phải là host này thì thông điệp được chuyển đến host phù hợp tại đó các giai đoạn tiếp theo của 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.

2. Giao thức Encapsulating Security Payload (ESP):

2.1 Cấu trúc gói tin ESP:

Hoạt động của ESP khác hơn so với AH, ESP đóng gói tất cả hoặc một phần dữ liệu gốc.



<table>
<tr><td>0 - 7 bit</td><td>8 - 15 bit</td><td>16 - 23 bit</td><td>24 - 31 bit</td></tr>
<tr><td colspan="4">Security parameters index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Payload data (variable)</td></tr>
<tr><td></td><td colspan="2">Padding (0-255 bytes)</td><td></td></tr>
<tr><td></td><td></td><td>Pad Length</td><td>Next Header</td></tr>
<tr><td colspan="4">Authentication Data (variable)</td></tr>
</table>

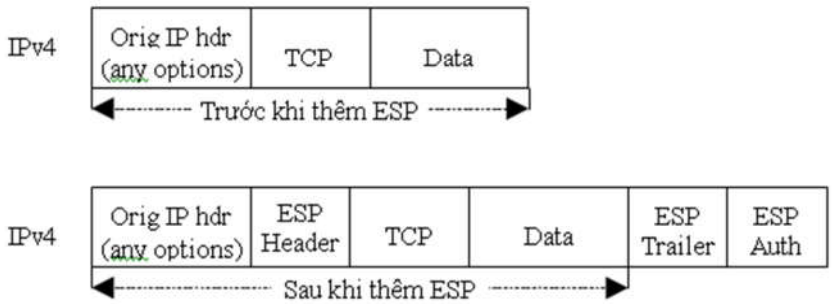
- Ý nghĩa các trường trong ESP :
  - SPI : Là một số 32 bit cùng với địa chỉ IP đích. Các giá trị SPI từ 1-255 được dành riêng để sử dụng trong tương lai.
  - Sequence Number : Tương tự như trong cấu trúc gói AH
  - Payload Data: Bao gồm một số các byte dữ liệu gốc hoặc một phần dữ liệu yêu cầu bảo mật đã được mô tả trong trường Next Header. Trường này được mã hóa bằng thuật toán mã hóa đã chọn trong quá trình thiết lập SA, thường sử dụng thuật toán DES-CBC, 3DES, CDMF
  - Padding: Nếu thuật toán mã hóa được sử dụng yêu cầu plaintext phải là số nguyên lần khối các byte. Ví dụ, trường hợp mã khối thì Padding được sử dụng để điền đầy vào plaintext(gồm Payload Data, Pad Length, Next Header và Padding) có kích thước theo yêu cầu. Có thể xem Padding như là phần đệm thêm.
  - Authentiaction data: Thông tin xác thực được tính trên toàn bộ gói ESP.

2.2 Quá trình xử lý ESP:

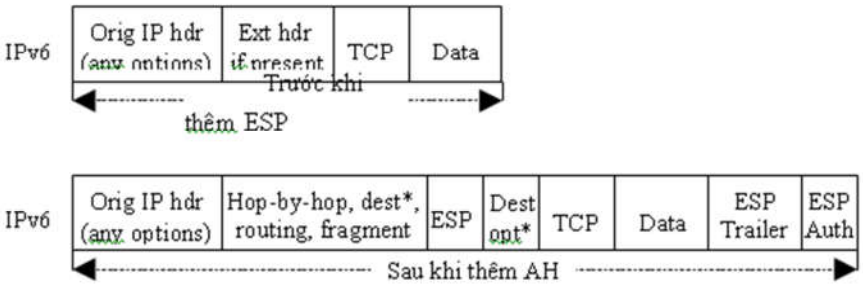
a. Vị trí của Header:

Ở Transport mode, ESP được chèn vào sau một IP header và trước một giao thức lớp trên (như TCP, UDP, ICMP). Đối với IPv4, ESP header đặt sau

IP header và trước giao thức lớp trên (TCP), ESP trailer bao gồm các trường Padding, Pad Length, Next header. Đối với IPv6, sau phần header mở rộng hop to hop, routing và fragmentation.

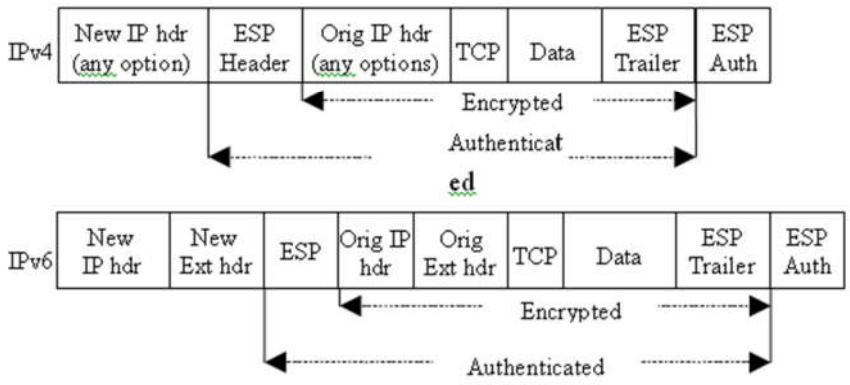


Khuông dạng IPv4 trước và sau khi xử lý ESP ở Transport mode



Khuông dạng IPv6 trước và sau khi xử lý ESP ở Transport mode.

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.



Khuông dạn gói tin đã xử lý ESP ở Tunnel mode

b. Các thuật toán:

Thuật toán được sử dụng với ESP thường là:

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

Đảm bảo ít nhất một trong hai dịch vụ bảo mật hoặc nhận thực phải được thực hiện, nên cả hai thuật toán xác thực và mã hóa không được đồng thời bằng NULL.

- Các thuật toán mã hóa: Thuật toán mã hóa được xác định bởi SA. ESP làm việc với các thuật toán mã hóa 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 để giải mã. Dữ liệu này được chỉ định trong trường Payload (ví dụ dưới dạng các vector khởi tạo) hoặc thu được từ header của gói.
- Các thuật toán xác thực: Thuật toán xác thực sử dụng để tính ICV, được xác định bởi SA. Đối với truyền thông point-to-point, các thuật toán xác thực thích hợp bao gồm các hàm băm một chiều MD5, SHA-1,…

c. Xử lý gói đầu ra:

Đối với Transport mode, phía phát đóng gói thông tin giao thức lớp trên và ESP header/trailer và giữ nguyên IP header. Đối với Tunnel mode, có thêm sự xuất hiện của outer IP header. Quá trình xử lý cụ thể như sau:

- Tìm kiếm SA: ESP được thực hiện trên một gói tin đầu ra chỉ khi quá trình IPSec xác định được gói tin đó đã liên kết với một SA, SA sẽ yêu cầu ESP xử lý gói tin.
- Mã hóa gói tin: Đối với Transport mode chỉ đóng gói thông tin giao thức lớp cao. Với Tunnel mode, đóng gói toàn bộ gói

IP ban đầu, thêm trường Padding nếu cần thiết, mã hóa các trường sử dụng khóa; thuật toán được quy định bởi SA và đồng bộ dữ liệu mã hóa nếu có.

- Tạo SN: Tương tự như trường hợp giao thức AH.
- Tính toán ICV: Nếu dịch vụ xác thực được chọn thì phía phát sẽ tính toán giá trị ICV trên dữ liệu gói ESP trừ trường Authentication Data. Các trường mã hóa được thực hiện trước xác thực. Chi tiết tính toán tương tự như ở AH.
- Phân mảnh: Phân mảnh được thực hiện sau khi đã xử lý ESP. Vì vậy ESP trong Transport mode 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 mà bị phân mảnh trong quá trình truyền qua các router trên đường truyền thì các mảnh phải được ghép lại trước khi xử lý ESP ở phía thu. Với Tunnel mode, ESP có thể được thực hiện trên gói IP mà phần Payload là 1 gói IP phân mảnh.

d. *Xử lý gói đầu vào.*

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

- 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. Thông tin trong SA sẽ cho biết cần phải kiểm tra trường Sequence Number hay không, cần thêm trường Authentication Data không, các thuật toán và khóa cần sử dụng để giải mã ICV nếu có. Nếu không tìm thấy SA nào phù hợp cho phiên truyền dẫn, phía thu sẽ loại bỏ gói này.
- Kiểm tra SN: ESP luôn hỗ trợ dịch vụ chống phát lại (anti-replay). Nếu dịch vụ xác thực không được chọn, Sequence Number không được bảo vệ tính toàn vẹn , dịch vụ anti-replay không thực hiện được. Nếu phía thu không chọn dịch vụ

chống phát lại, thì không cần kiểm tra Sequence Number. Nếu phía thu chọn dịch vụ chống phát lại thì bộ đếm gói thu được khởi tạo là 0 khi thiết lập SA. Với mỗi gói thu được, phía thu phải kiểm tra rằng gói đó có chứa số Sequence Number không lặp của bất kỳ một gói nào trong thời gian tồn tại SA đó.

- Kiểm tra ICV: Nếu dịch vụ xác thực được lựa chọn, phía thu sẽ tính ICV dựa trên dữ liệu gói ESP, trừ trường AD, sử dụng thuật toán xác thực được xác định trong SA và so sánh với giá trị ICV trong trường Authentication của gói. Nếu 2 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 này. Việc kiểm tra cụ thể như sau: Giá trị ICV nằm trong trường Authentication Data được tách khỏi gói ESP và được lưu trữ tạm. Tiếp theo kiểm tra độ dài của gói ESP(trừ trường AD vừa tách). Nếu Padding ngầm định được yêu cầu bởi thuật toán xác thực thì các byte 0 được thêm vào cuối gói ESP, sau trường Next Header. Thực hiện tính toán ICV và so sánh với giá trị đã lưu trữ tạm.

e. <u>Giải mã gói:</u>

Nếu ESP sử dụng mã hóa thì sẽ phải thực hiện quá trình giải mã. Quá trình giải mã như sau:

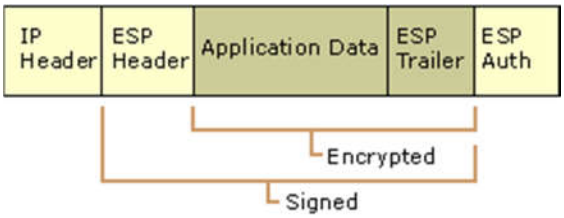
- Giải mã ESP (bao gồm trường Payload Data, Padding, Pad Length, Next header) sử dụng khóa. Thuật toán mã hóa được xác định bởi SA.
- Xử lý phần Padding theo đặc tả của thuật toán. Phía thu cần tìm và loại bỏ phần Padding trước khi chuyển dữ liệu đã giải mã lên lớp trên.
- Xây dựng lại cấu trúc gói IP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

Có các lý do dẫn đến quá trình giải mã không thành công:

- SA được lựa chọn không đúng. SA có thể sai các thông số SPI, IP đích.
- Độ dài phần Padding hoặc giá trị của nó bị sai.
- Gói ESP mã hóa bị lỗi.

Chữ ký và mã hóa

Như phần trên đã nói, ESP mang lại sự bảo vệ cho các giao thức ở các lớp trên của nó. Hình sau đây cho ta thấy phần nào của ESP sẽ giúp nó thực hiện nhiệm vụ đảm bảo tính toàn vẹn của dữ liệu và phần nào là phần mã hóa thực hiện nhiệm vụ bảo mật dữ liệu.



"Chữ ký và mã hóa" (Nguồn: http://technet.microsoft.com/en-us/library/cc959510.aspx)

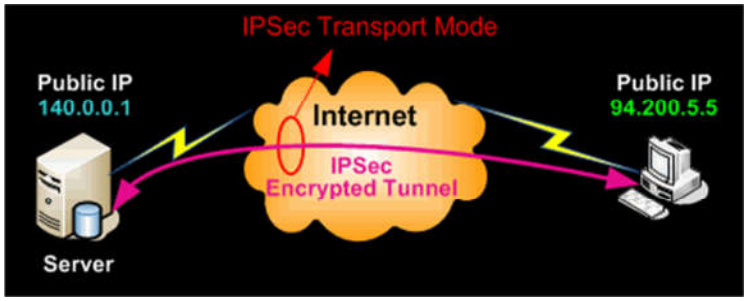
C. Phương thức kết nối trong Phase 2:

Như đã đề cập trong các phần trên, có hai cách mà AH và ESP có thể sử dụng để truyền thông tin bảo mật đến đích:

- Transport mode
- Tunnel mode

1. Transport mode :

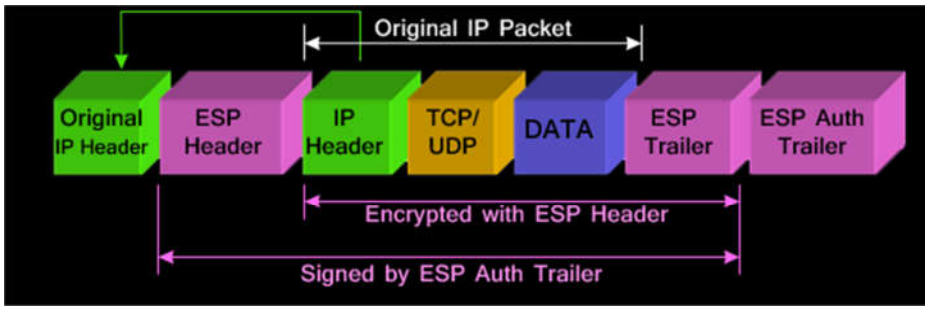
Transport mode được sử dụng giữa hai thiết bị nguồn và đích đầu cuối thực sự (để phân biệt với trường hợp Tunnel Mode), tức là kết nối end-to-end, chính các thiết bị này sẽ thực hiện các dịch vụ bảo vệ cho dữ liệu.



IPsec Transport Mode

Transport mode bảo vệ cho IP Payload, tức là bao gồm TCP/UDP Header và dữ liệu qua việc sử dụng AH hoặc ESP. Trong mode này, IP Header ban đầu sẽ giữ nguyên không đổi, chỉ có trường protocol là thay đổi từ số 50 (ESP) hay 51 (AH). Mode này thường được sử dụng để bảo vệ cho một giao thức đường hầm khác, chẳng hạn như GRE, GRE đầu tiên sẽ đóng gói gói tin IP, sau đó IPsec sẽ bảo vệ cho gói tin GRE đó.

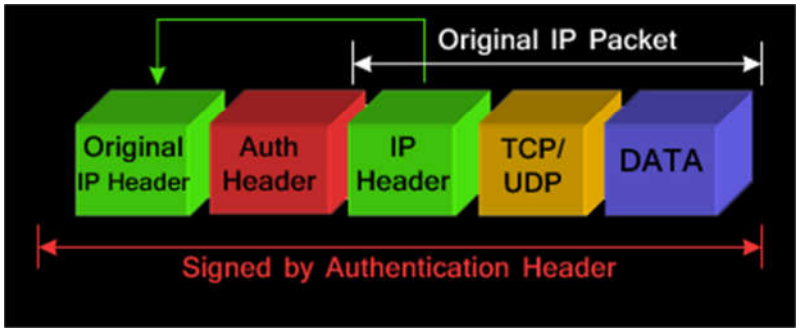
Gói tin với giao thức ESP được chỉ ra trong hình sau:



Gói tin ESP trong Transport Mode (Nguồn: http://www.firewall.cx/networking-topics/protocols/870-IPsec-modes.html)

Lưu ý rằng IP Header ở phía trước chính là gói IP ban đầu. Việc đặt gói này ở đầu cho ta thấy Transport Mode không mang lại sự bảo vệ hoặc mã hóa cho IP Header ban đầu.

Gói tin với giao thức AH được chỉ ra trong hình sau:



AH có thể hoạt động độc lập hoặc kết hợp với ESP khi IPsec được sử dụng trong Transport Mode. Việc của AH là bảo vệ cho cả gói tin, tuy nhiên, IPsec trong transport mode không hề tạo ra một IP Header mới ở đầu gói tin mà lại sao chép nguyên IP Header gốc ra bên ngoài, có thay đổi cũng chỉ là thay đổi protocol ID sang 51.

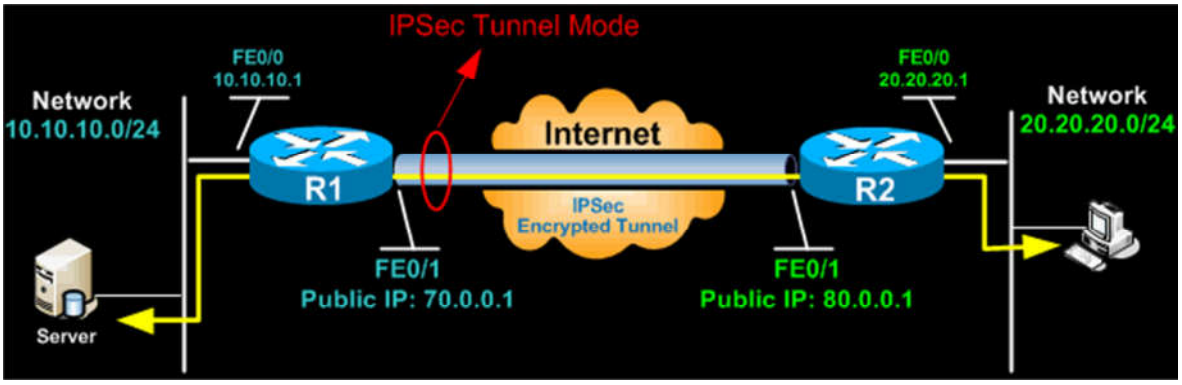
Tóm lại, trong IPsec transport mode, đối với cả ESP và AH, IP Header đều bị lộ.

2. Tunnel mode:

Đây chính là mode mặc định của VPN. Với mode này, cả gói tin IP ban đầu sẽ được bảo vệ. Nghĩa là IPsec sẽ lấy cả gói tin ban đầu, mã hóa nó, thêm một IP Header mới và gửi nó tới đầu kia của "tunnel".

Mode này được sử dụng phổ biến giữa các gateway (Cisco routers, ASA firewalls), gateway lúc này hoạt động giống như là một proxy cho thiết bị đằng sau nó. Do đó, đối với Tunnel mode, những thiết bị đích và nguồn không thực hiện dịch vụ bảo mật cho dữ liệu người dùng mà chính những thiết bị trung gian sẽ làm chuyện này.

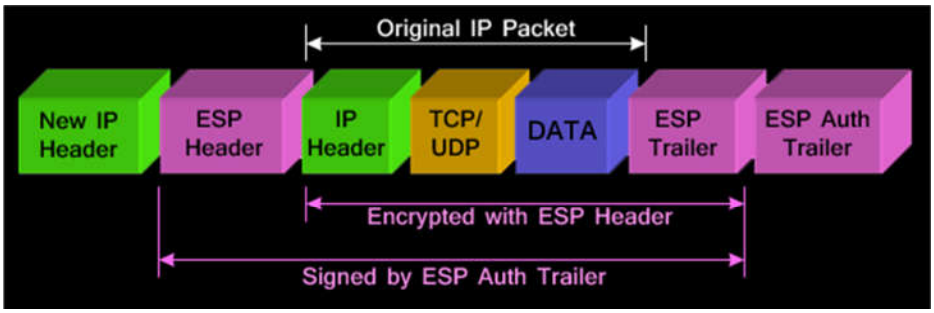
Cách này được sử dụng cho kết nối site-to-site và kết nối truy cập từ xa. Gói IP gốc ban đầu chứa thông tin về đầu cuối thực sự lúc này được bảo vệ và đóng vào trong thông tin của AH/ESP, sau đó một IP Header khác chứa địa chỉ của các thiết bị trung gian được gắn thêm vào gói tin, do đó thông tin về đầu cuối thực sự hoàn toàn được bảo mật nhưng không làm ảnh hưởng đến việc định tuyến gói tin. Những thuận lợi chính của Tunnel mode so với loại Transport mode là dịch vụ bảo mật tập trung trên số lượng thiết bị nhỏ hơn (chủ yếu chỉ là các thiết bị trung gian), do đó tạo thuận lợi cho việc cấu hình và quản lí.



)

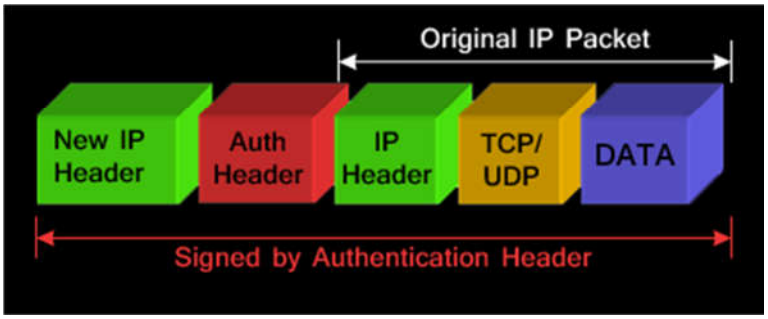
Trong tunnel mode, IPsec Header (AH hoặc ESP Header) sẽ được chèn giữa phần IP Header và phần giao thức lớp trên. Giữa AH và ESP, ESP được sử dụng phổ biến hơn trong cấu hình IPsec VPN Tunnel.

Cấu trúc gói tin dùng giao thức ESP trong IPsec tunnel mode như hình sau:



)

Cấu trúc gói tin dùng giao thức AH trong IPsec tunnel mode như hình sau:



)

Kết thúc phần này, ta rút ra một điều sau đây: transport mode chỉ sử dụng trong những ***kết nối chỉ cần dữ liệu được bảo vệ (chẳng hạn kết nối dùng giao thức TFTP để lấy file cấu hình, hoặc kết nối để các máy nội bộ upload***

file log hệ thống lên server, …). Do vậy, để có thể bảo vệ được cả phần IP Header chứa thông tin đầu cuối của thiết bị, ta phải sử dụng tunnel mode, trong tunnel mode, giao thức ESP được sử dụng phổ biến hơn do tính tương thích với dịch vụ NAT của nó.

D. Phase 2 Transforms:

Dạng biến đổi dữ liệu (Data Transform) định nghĩa cách mà kết nối dữ liệu được bảo vệ. Cũng giống như kết nối quản lý được trình bày ở phần Phase 1, kết nối dữ liệu trong ISAKMP/IKE phase 2 cũng cần phải được định nghĩa dạng của nó như thế nào để bảo vệ dữ liệu người dùng một cách tốt nhất. Dạng biến đổi của dữ liệu bao gồm những thông tin sau:

- Giao thức bảo mật: AH và ESP.
- Loại kết nối cho giao thức bảo mật: Tunnel hoặc Transport Mode.
- Thông tin mã hóa (chỉ riêng với ESP): DES, 3DES, AES-128.AES-192, AES-256 hoặc không dùng thuật toán mã hóa nào.
- Các hàm HMAC để chứng thực: MD5 hoặc SHA-1 (ESP có thể dùng hoặc không).

E. Kết nối dữ liệu:

Để tạo được kết nối dữ liệu, hai thiết bị đầu cuối phải thương lượng các phương thức bảo mật dữ liệu sao cho thống nhất với nhau. Khi ISAKMP/IKE Phase 1 hoàn tất, hai thiết bị đã có một kết nối quản lý để có thể liên lạc được với nhau thông qua các thông điệp ISAKMP/IKE. Do đó, các thiết bị sẽ dùng kết nối này để đàm phán với nhau trong việc thiết lập Phase 2. Mỗi thiết bị sẽ chia sẻ những thông tin sau đây với thiết bị kia:

- Đường kết nối nào cần được bảo vệ.
- Danh sách các thông tin Data Transform cần để bảo vệ đường đó, chẳng hạn như giao thức bảo mật, hàm HMAC, thuật toán mã hóa, …
- Địa chỉ IP được sử dụng ở IP Header ngoài cùng của gói tin.
- Thời gian sống tính theo giây hay KBs.

Ta hãy xem một ví dụ sau đây, có 2 thiết bị IPsecA và IPsecB, mỗi thiết bị lại có một Transform khác nhau.

IPsecA có các thông tin sau đây:

1. Transform 1A: AH với MD5, ESP với AES-256, tunnel mode.
2. Transform 2A: ESP với MD5, ESP với AES-128, tunnel mode.

IPsecB có các thông tin sau đây:

1. Transform 1B: ESP với MD5, ESP với AES-128, tunnel mode.
2. Transform 2B: ESP với MD5, ESP với 3DES, tunnel mode.

Các Transform đó sẽ lần lượt được so sánh với nhau cho tới khi chúng giống nhau hoàn toàn. Một kết nối dữ liệu sẽ được tạo ra. Ta lưu ý rằng đối với một số nhà cung cấp thiết bị, thời gian sống của 2 thiết bị thì không cần thiết phải giống nhau, chúng sẽ tự động chọn giá trị lifetime nhỏ nhất.

V. IPSEC OVER TCP/UDP :

A. Vấn đề chuyển đổi địa chỉ trong IP Sec:

Phần này nghiên cứu về vấn đề chuyển đổi địa chỉ trong IPsec.

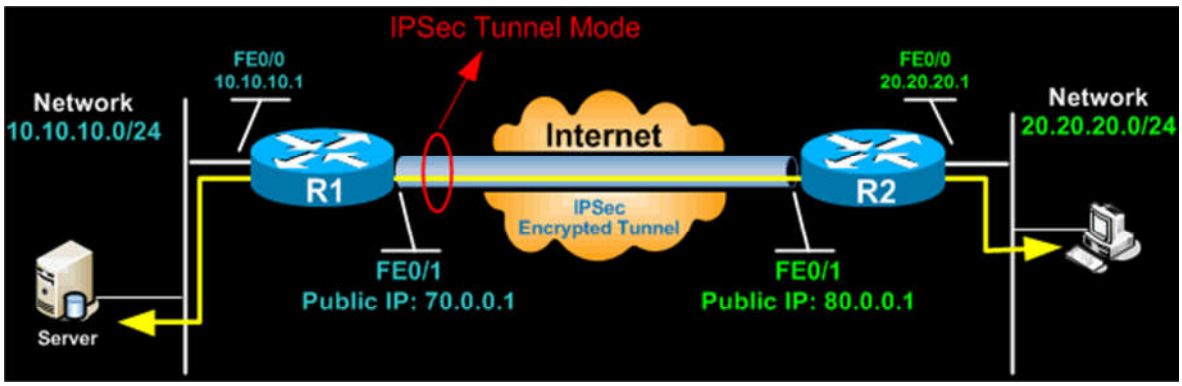
Vấn đề chuyển đổi địa chỉ là một trong hai vấn đề quan trọng cần phải được giải quyết trong đường truyền IPsec bên cạnh vấn đề Firewall.

Như ta đã biết có hai loại kết nối trong IPsec là kết nối quản lý (management connection) và kết nối dữ liệu (data connection). Những thiết bị thực hiện việc chuyển đổi địa chỉ không gây ra vấn đề gì cho kết nối quản lý, nhưng đối với kết nối dữ liệu thì ngược lại. Trường hợp ngoại lệ là trước đây một số thiết bị sử dụng PAT sẽ buộc tất cả kết nối quản lý phải sử dụng giao thức UDP với port 500 cho cả nguồn và đích, gây ra một số vấn đề nếu ta sử dụng nhiều kết nối song song cùng lúc thông qua thiết bị PAT; nhờ việc cải tiến công nghệ nên các thiết bị hiện nay đều đã khắc phục được vấn đề này. Sau đây ta sẽ xem ảnh hưởng của việc chuyển đổi địa chỉ với việc kết nối dữ liệu trong IPsec.

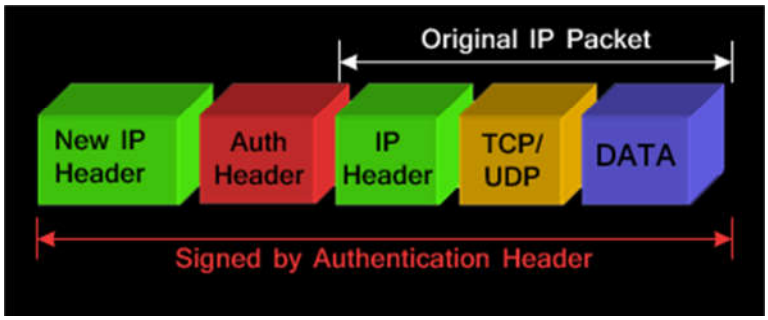
Như đã đề cập trong phần "ISAKMP/IKE giai đoạn 2", AH hoàn toàn không hoạt động khi việc chuyển đổi địa chỉ được thực hiện trên một gói tin AH. Cả PAT và NAT đều không hỗ trợ truyền gói tin có chứa AH này. Đối

với NAT, nó sẽ thực hiện việc chuyển đổi địa chỉ IP của nguồn và đích, trong khi gói tin AH chứa các giá trị hàm băm của hầu hết các trường trong gói tin IP ban đầu phục vụ cho việc bảo mật hoặc chứng thực. Đối với PAT, do AH là giao thức lớp 3 nên nó sẽ không thêm phần TCP/UCP Header mà PAT cần nên AH không thể tương thích với PAT. Sau đây ta sẽ chứng minh rõ hơn phần này dựa vào hình vẽ.

Ta sử dụng tunnel mode vì đây là mode mặc định cũng như nó tương ứng với việc các thiết bị trung gian chính là các thiết bị thực hiện NAT hoặc PAT.

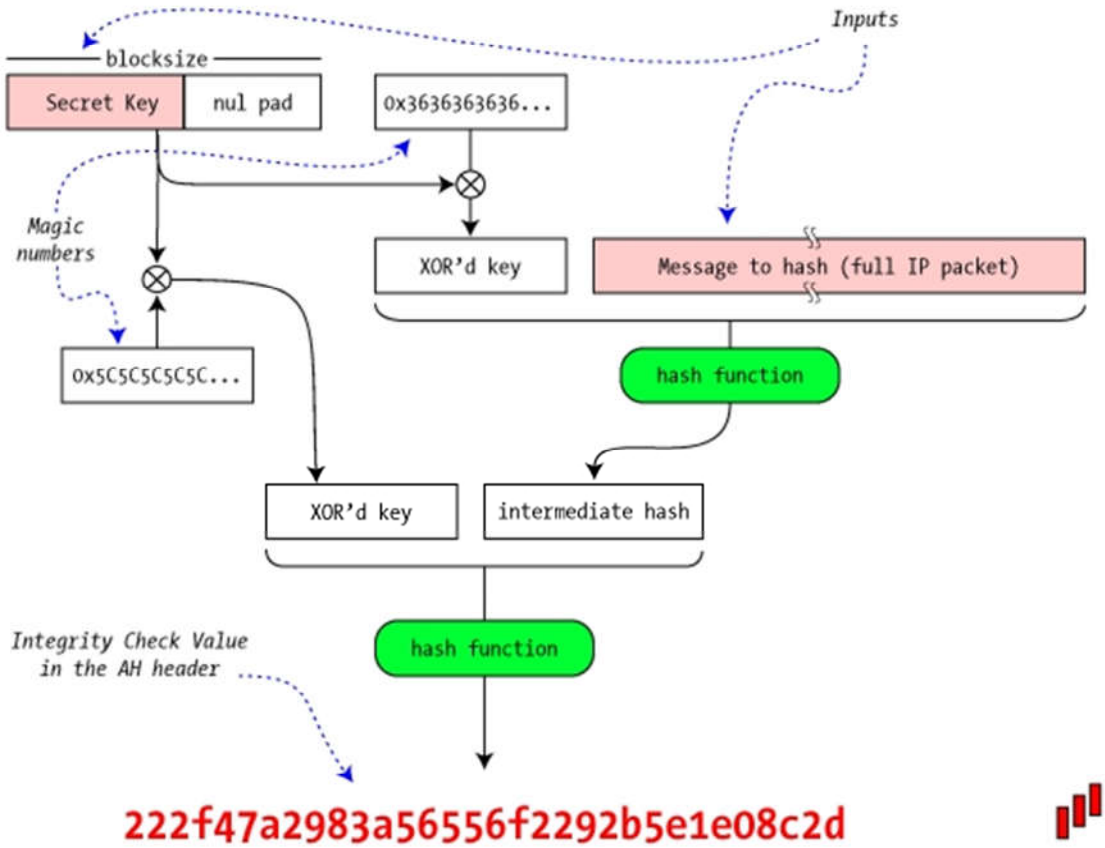


Đối với giao thức AH. Gói tin của nó sẽ có cấu trúc như sau:



)

Ta thấy rằng tất cả các phần bao gồm gói tin IP ban đầu (tức là của thiết bị đầu cuối thực sự) và phần IP Header mới được gắn vào đều được "signed by AH". Tức là AH Header sẽ chứa mã được sinh ra từ một hàm băm phục vụ cho việc chứng thực dữ liệu tại thiết bị nhận. Mã băm này được sinh ra từ các thành phần gói IP ban đầu và IP Header mới. Ta quan sát hình sau để hiểu rõ hơn về cơ chế này.



Quá trình tạo AH Header (Input bao gồm gói IP ban đầu và IP Header mới, secret key đã được *chia sẻ trước đó thông qua kết nối quản lý) (Nguồn:*

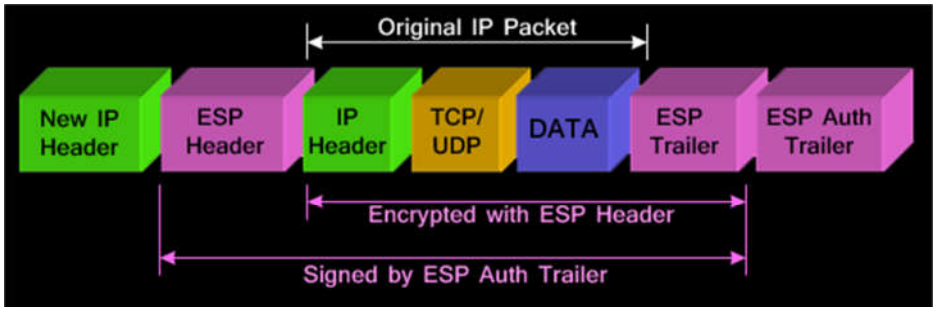
Tại đầu thu, thiết bị đích cũng sẽ tạo ra một mã băm với input là các thông tin như các thông tin được tạo mã băm ở đầu thu. Sau đó, nó so sánh với mã băm nhận được nằm trong AH Header (ICV). Nếu giống nhau, dữ liệu được chứng thực toàn vẹn, ngược lại, dữ liệu được coi là không toàn vẹn.

Phần trên là những công đoạn mặc định của giao thức AH. Tuy nhiên, khi ta sử dụng dịch vụ NAT, mọi chuyện sẽ khác. Ta để ý rằng cả IP Header mới cũng được bao gồm trong quá trình tính toán AH Header. Bước tiếp theo, NAT được thực hiện trên gói tin này, nó sẽ thay đổi địa chỉ IP đầu và cuối trong IP Header mới trong khi phần AH Header vẫn không bị thay đổi. Đúng như bước tiếp theo, khi gói tin được thiết bị thu nhận được, nó sẽ tạo mã băm và so sánh với mã băm nhận được nằm trong AH Header. Lúc

này, hai mã băm sẽ không giống nhau, gói tin sẽ được xem là giả mạo và bị drop ngay lập tức.

Tiếp tục với PAT, PAT cần thay đổi số port trên TCP/UDP Header của gói tin. Tuy nhiên, AH là một giao thức lớp 3, phần TCP/UDP Header thực hiện ở lớp 4 đối với AH đã được coi như là dữ liệu người dùng, vì vậy gói tin coi như không có TCP/UDP Header và PAT không thể thực hiện được nhiệm vụ của nó.

Đối với giao thức ESP, gói tin của nó có cấu trúc như sau:



)

Các bước diễn ra việc chứng thực giống hệt như giao thức AH. Tuy nhiên, phần IP Header mới không được "signed by ESP Auth Trailer", nó không bao gồm trong khi tính toán ICV, chỉ ESP Header (và cả ESP trailer nếu có) và dữ liệu người dùng (gói IP ban đầu) là được bao gồm trong tính toán ICV mà thôi, và do đó ESP hoàn toàn tương thích với NAT.

Tuy nhiên, cũng với một lý do giống như AH, ESP cũng không tương thích với PAT.

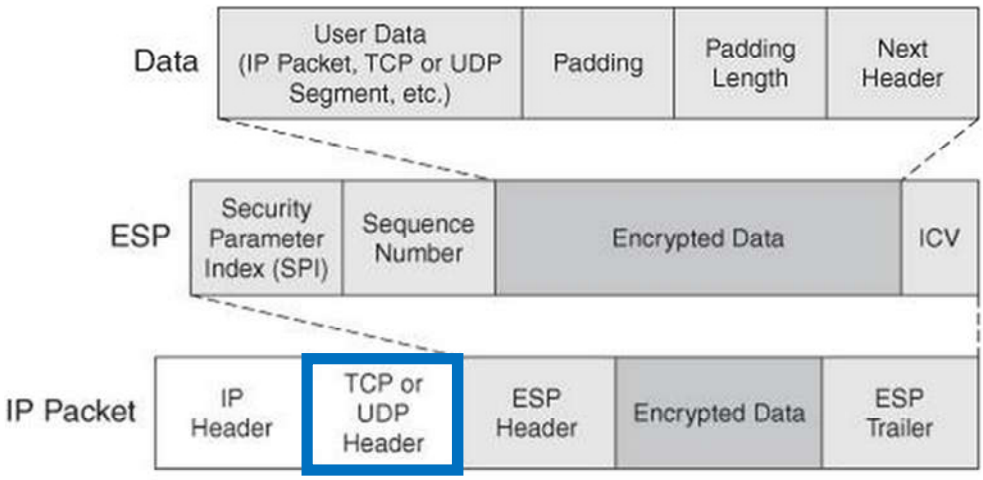
B. Giải quyết vấn đề chuyển đổi địa chỉ trong IP Sec:

Có nhiều giải pháp đã được đề xuất để giải quyết vấn đề chuyển đổi địa chỉ trong IPsec. Một trong những phương pháp phổ biến nhất đó là luôn sử dụng giao thức đóng gói ESP thay vì sử dụng AH. Như phần trên ta đã biết rằng ESP thì hoạt động với NAT, nhưng không hoạt động với PAT. Do đó vấn đề của chúng ta là làm sao để ESP hoạt động được với những thiết bị thực hiện PAT.

Comparisons	NAT-T	IPsec over UDP	IPsec over TCP
Standard versus proprietary	RFC	Cisco	Cisco
Encapsulation method	UDP	UDP	TCP
When encapsulation is done	Tested	Always	Always

Nhiều giải pháp đã được đề xuất trong đó có NAT-T cũng là một trong những cách phổ biến (Nguồn: The Complete Cisco VPN Configuration Guide – Richard Deal)

Để làm được điều này, người ta sẽ chèn một phần Header TCP hoặc UDP giữa phần IP Header bên ngoài và phần ESP giống như hình sau đây:



Giải quyết vấn đề chuyển đổi địa chỉ trong IPsec (Nguồn: The Complete Cisco VPN Configuration Guide – Richard Deal)

Do phần TCP/UDP Header này thuộc phần Header bên ngoài nên nó sẽ không bao gồm trong quá trình tính toán mã băm để tạo chữ ký số.

Đối với IPsec over UDP, một UDP Header chuẩn luôn luôn được chèn vào giữa phần IP Header bên ngoài và phần ESP Header. Việc này giúp ESP giải quyết vấn đề với PAT. Tuy nhiên nó mắc một khuyết điểm, đó là thiết bị luôn luôn thực hiện việc chèn này cả trong trường hợp không có thiết bị chuyển đổi địa chỉ nào giữa hai đầu cuối, lúc này phần UDP Header trở nên dư thừa.

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

(Nguồn: wikipedia)

Đối với IPsec over TCP, một Header TCP sẽ được chèn vào giữa phần IP Header bên ngoài và phần ESP Header. Tuy nhiên, nhược điểm của loại này so với IPsec over UDP là phần TCP Header chứa nhiều bytes hơn UDP Header. Cũng vì nhược điểm đó nên TCP header thường được ít sử dụng hơn so với UDP header.

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset			Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if Data Offset > 5, padded at the end with "0" bytes if necessary) ...																															

(Nguồn: wikipedia)

Lưu ý: để biết được sự tồn tại của NAT giữa hai hosts trong một mạng nào đó, IPsec có cơ chế như sau: hai thiết bị sẽ gửi thông tin của địa chỉ IP (nguồn và đích) và các số port cũng với mã băm của các thông tin đó cho nhau, nếu cả hai thiết bị đó tính toán mã băm và thu được cùng kết quả với mã băm nhận được, chúng sẽ biết là không có NAT ở giữa. Ngược lại, nếu mã băm không giống nhau, tức là đã có sự thay đổi địa chỉ IP hoặc số port, khi đó hai thiết bị phải thực hiện đóng gói gói tin trong UDP hoặc TCP Header để có thể sử dụng được IPsec.

Sau khi chèn phần TCP/UDP Header vào gói tin, một số thông tin của gói tin có thể bị thay đổi, do đó bước đóng gói hoàn chỉnh của IPsec over UDP phải như sau:

1) Thực hiện quá trình đóng gói ESP.
2) Chèn một UDP Header đã được định chuẩn một cách hợp lý vào gói tin.
3) Điều chỉnh lại các trường Total Length, Protocol và Header Checksum (đối với Ipv4) trong phần IP Header mới làm sao cho đúng với gói IP mới được tạo ra.

Tương tự, quá trình giải gói cũng được thực hiện theo từng bước sau đây:

1) Loại bỏ phần UDP Header khỏi gói tin.
2) Thực hiện quá trình giải gói ESP (bao gồm việc chứng thực, …)
3) Thực hiện quá trình NAT trong tunnel mode để trả về gói tin IP gốc ban đầu.