Trường Đại Học Khoa Học – Đại Học Huế

Khoa Công Nghệ Thông Tin

---\*\*\*---



**TIỂU LUẬN AN NINH MẠNG**

**ĐỀ TÀI: TÌM HIỂU VÀ TRIỂN KHAI IPSEC VPN VỚI PHẦN MỀM GIẢ LẬP GNS3**

**Lớp tín chỉ: 2024-2025.1.TIN3163.006**

**Số tín chỉ: 3**

**Giáo viên hướng dẫn: ThS.Võ Việt Dũng**

**Nhóm thực hiện: Nhóm 7**

**Hồ Văn Diễn Lương Thanh Ngọc Như**

**Nguyễn Văn Phong Nguyễn Văn Tiến Đạt**

**Bùi Khắc Hiếu Nguyễn Công Nhân**

**Ngô Trần Thuận Khang**

**Huế, ngày 18 tháng 12 năm 2024**

**MỤC LỤC**

**Lời mở đầu .......................................................................................................... 4**

**I. Tìm hiểu về IPSec .......................................................................................... 5**

1. **Giới thiệu về IPSec ............................................................................... 5**
2. **Kiến trúc giao thức IPSec .................................................................... 5**
   1. Mô hình chung ................................................................................... 5
   2. Các giao thức cơ bản .......................................................................... 6
   3. Liên kết bảo mật ................................................................................. 6
   4. Transport mode và Tunnel mode ......................................................... 6
3. **Giao thức AH ........................................................................................ 7**
   1. Các cơ chế bảo vệ được cung cấp bởi giao thức AH ............................. 7
   2. Cấu trúc của AH ................................................................................ 7
   3. Vị trí của AH ..................................................................................... 8
   4. Các mode làm việc trong AH .............................................................. 9
   5. Nested và Adjacent header trong AH ................................................... 9
   6. Quá trình xử lý tiêu đề của IPSec ...................................................... 10
   7. Quá trình xử lý của AH với các gói tin Outbound ............................... 10
   8. Quá trình xử lý của AH với các gói tin Inbound .................................. 14
   9. Một số điểm phức tạp trong giao thức AH ........................................... 15
4. **Giao thức ESP ..................................................................................... 21**
   1. Các cơ chế bảo vệ được cung cấp bởi ESP..................................... 21
   2. Cấu trúc của ESP......................................................................... 22
   3. Vị trí và các mode làm việc của ESP............................................ 24
   4. Nested và Adjacent header trong ESP........................................... 25
   5. Quá trính xử lý của ESP đối với gói tin Outbound ........................ 28
   6. Quá trính xử lý của ESP đối với gói tin Inbound .......................... 30
   7. Một số điểm phức tạp trong giao thức ESP .................................. 30
   8. Một số đánh giá, phê bình của các chuyên gia về ESP .................. 30
   9. Lý do sử dụng hai tiêu đề bảo vệ ................................................. 31

**II.Tìm hiểu về VPN ......................................................................................... 31**

**1. Khái niệm VPN .................................................................................... 31**

**2. Các mô hình triển khai ........................................................................ 31**

2.1. VPN Site-to-Site (Mạng-tới-Mạng) ........................................................ 31

2.2. VPN Client-to-Site (Máy khách-tới-Mạng) ............................................ 31

2.3. VPN cá nhân (cho người dùng cá nhân) ................................................. 32

**III.Triển khai hệ thống IPSec VPN trên phần mềm giả lập GNS3 ...... 32**

**1. Triển khai hệ thống VNP INPEC site to site ..................................... 32**

**2. Triển khai hệ thống VPN IPSEC client to site .................................. 36**

**IV.Tài liệu tham khảo .....................................................................................**

**LỜI MỞ ĐẦU**

Trong thời đại công nghệ số và Internet phát triển mạnh mẽ như hiện nay, các dịch vụ trực tuyến như đào tạo từ xa, mua sắm trực tuyến hay tư vấn y tế qua mạng đang trở thành những phần không thể thiếu trong cuộc sống hàng ngày. Tuy nhiên, sự phát triển mạnh mẽ của Internet cũng kéo theo không ít vấn đề về bảo mật và an toàn thông tin. Do tính chất toàn cầu và không bị kiểm soát bởi bất kỳ tổ chức hay chính phủ nào, Internet dễ dàng trở thành mục tiêu cho các hành vi xâm nhập trái phép, tấn công mạng hoặc đánh cắp dữ liệu. Chính vì thế, các biện pháp bảo mật trở thành yếu tố vô cùng quan trọng để đảm bảo rằng thông tin, dữ liệu trao đổi qua mạng luôn được bảo vệ an toàn.

Trong bối cảnh đó, mạng riêng ảo (Virtual Private Network – VPN) ra đời như một giải pháp hiệu quả giúp giải quyết những vấn đề trên. VPN giúp tạo ra một kết nối an toàn, mã hóa thông tin trên đường truyền công cộng, qua đó tạo ra một "đường ống bảo mật" giữa hai điểm đầu cuối, bảo vệ dữ liệu không bị rò rỉ hoặc xâm nhập trong suốt quá trình truyền tải. Một trong những giao thức quan trọng nhất trong việc xây dựng một hệ thống VPN là IPSEC (Internet Protocol Security). IPSEC cung cấp các cơ chế bảo mật mạnh mẽ, từ việc mã hóa dữ liệu đến xác thực các gói tin, đảm bảo rằng tất cả các thông tin truyền tải đều được bảo vệ nghiêm ngặt.

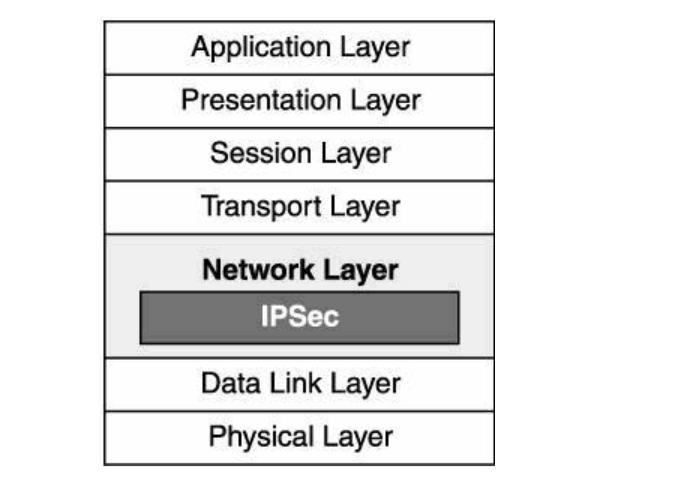
Bằng cách triển khai IPSEC, các tổ chức và cá nhân có thể thiết lập các mạng riêng ảo một cách an toàn, ngay cả khi sử dụng hạ tầng mạng công cộng, từ đó đảm bảo tính bảo mật trong các giao dịch trực tuyến. Việc hiểu rõ các khái niệm cơ bản và cách thức hoạt động của IPSEC sẽ giúp chúng ta nắm bắt và áp dụng các biện pháp bảo mật hiệu quả trong môi trường mạng. Hơn nữa, thông qua việc mô phỏng hệ thống IPSEC/VPN trên phần mềm giả lập như GNS3, chúng ta có thể hiểu rõ hơn về cách thức triển khai và vận hành các giải pháp bảo mật mạng trong thực tế.

**I. Tìm hiểu về IPSEC**

**1. Giới thiệu về IPSEC**

IPSEC (Internet Protocol Security) là giao thức ở lớp Network (OSI) cho phép gửi nhận các gói IP được mã hóa. Tùy theo mức độ cần thiết, IPSEC có thể cung cấp cả tính bảo mật và xác thực cho quá trình trao đổi dữ liệu dựa trên hai kiểu dịch vụ mã hóa: AH, ESP.

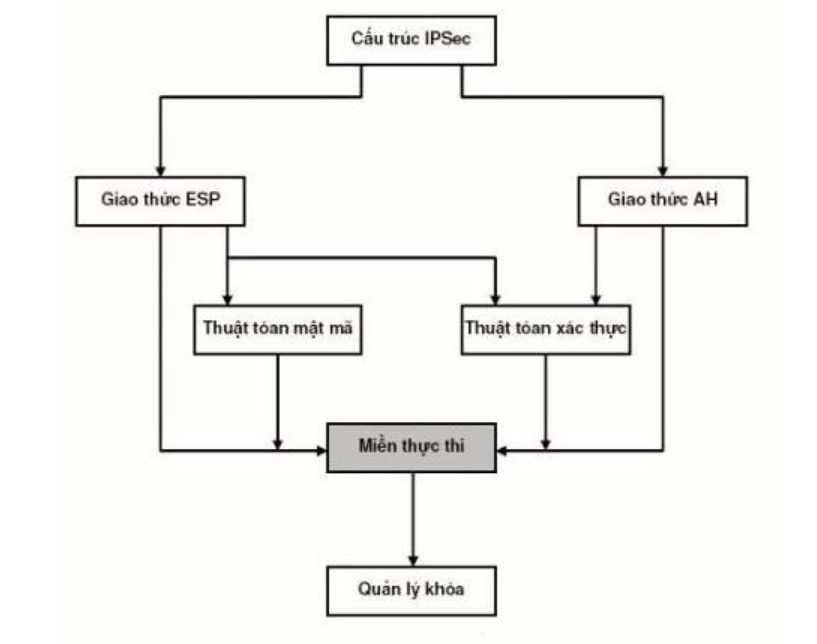
Mục đích chính của việc phát triển IPSEC là cung cấp một cơ cấu bảo mật ở tầng 3 trong mô hình OSI.



IPSEC cũng là một thành phần quan trọng hỗ trợ giao thức L2TP (Layer two tunnelin) trong công nghệ mạng riêng ảo VPN.

**2. Kiến trúc giao thức IPSEC:**

**2.1 Mô hình chung:**



**2.2 Các giao thức cơ bản trong IPSEC:**

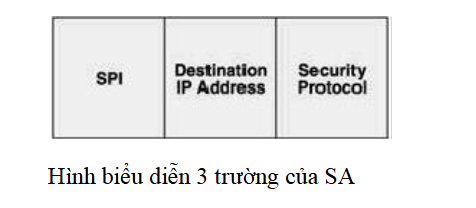
Hai giao thức cơ bản để thực thi IPSEC là AH và ESP.

AH chỉ cung cấp các dịch vụ xác thực, ESP vừa cung cấp các dịch vụ bảo mật vừa cung cấp các dịch vụ xác thực

**2.3 Liên kết bảo mật:**

SA (Security Associations): Là một khái niệm cơ bản của bộ giao thức IPSEC. SA là một kết nối luận lý theo một phương hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSEC.

- SA gồm có 3 trường:

****

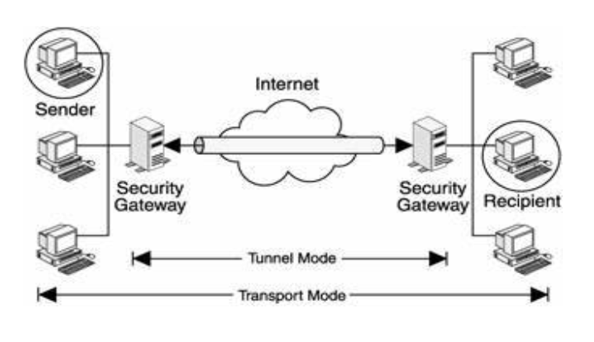
+ SPI (Security Parameter Index): là một trường 32 bits dùng nhận dạng giao thức bảo mật, được định nghĩa bởi trường Security protocol, trong bộ IPSEC đang dùng. SPI như là phần đầu của giao thức bảo mật và thường được chọn bởi hệ thống đích trong suốt quá trình thỏa thuận của SA.

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

+ Security protocol: mô tả giao thức bảo mật IPSEC, là AH hoặc là ESP.SA trong IPSEC được triển khai bằng 2 chế độ đó là Tunnel mode và Transport mode.

**2.4 Transport mode và Tunnel mode:**

Hiện tại, IPSEC có hai chế độ làm việc: Transport Mode và Tunnel Mode. Cả AH và ESP đều có thể làm việc với một trong hai chế độ này

 **Hình minh họa hai chế độ làm việc của ISPEC**

**3. Giao thức AH**

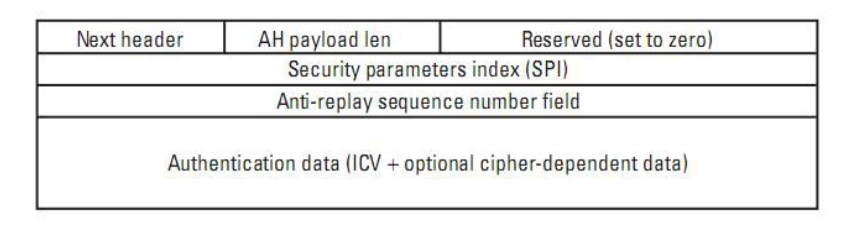
**3.1 Các cơ chế bảo vệ được cung cấp bởi giao thức AH:**

**Tính toàn vẹn thông tin (intergrity):** Cơ chế này đảm bảo gói tin nhận được chính là gói tin đã gửi.

**Xác thực nguồn gốc thông tin:** Cơ chế này đảm bảo gói tin được gửi bởi chính người gửi ban đầu mà không phải là người khác.

**Cơ chế chống phát lại (Replay protection) (đây là cơ chế tùy chọn (optional), không bắt buộc):** Cơ chế này đảm bảo rằng một gói tin không bị phát lại nhiều lần. Cơ chế này là một thành phần bắt buộc đối với bên gửi tuy nhiên bên nhận có thể tùy chọn sử dụng hoặc không sử dụng.

**3.2 Cấu trúc của AH:**

****

**Tiêu đề AH bảo vệ tính toàn vẹn của gói tin**

**Các trường trong AH:**

- **Next header (8 bits):** Xác định loại dữ liệu chứa trong tiêu đề AH. Sử dụng các quy ước của TCP/IP.

- **Payload len (8 bits):** Xác định độ dài tiêu đề AH, tính bằng đơn vị từ I(32 bits) trừ đi 2 đơn vị.

- **Reserved (16 bits):** Dành riêng chưa sử dụng, được gán chuỗi bit 0.

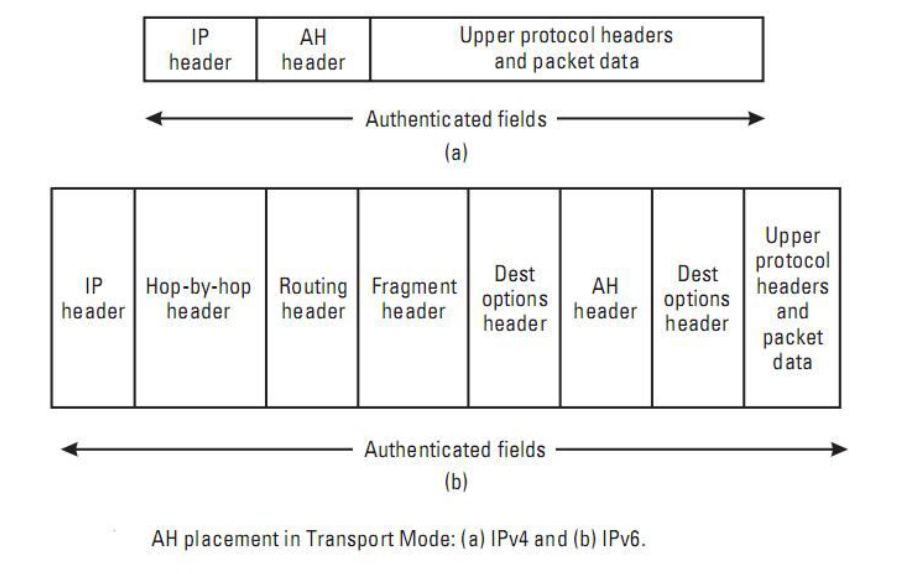
- **SPI (security paramaters index) (32 bits):** Nhận dạng liên kết SA. Giá trị từ 1 đến 255 được giành riêng. Giá trị 0 được dùng vào mục đích đặc biệt. Ví dụ một cơ chế quản lí khóa có thể sử dụng SPI với giá trị 0 để thể hiện rằng không có một SA nào tồn tại trong quá trình IPSEC đã yêu cầu bộ quản lí khóa tạo một SA mới nhưng SA này vẫn chưa được khởi tạo.

- **Sequence number (32 bits):** Số thứ tự gói truyền trên SA. Thông qua việc theo giỏi chỉ số này và gửi nó cho bên nhận, bên gửi có thể giúp bên nhận thực hiện việc chống phát lại (anti-replay) nếu bên nhận muốn.

- **Authentication data:** Trường này có kích thước không xác định, không xác định trước, đảm nhiệm vai trò chính của AH. Nó bao gồm ICV (intergrity check value: kiểm tra sự toàn vẹn). Bên nhận sử dụng nó để kiểm tra tính toàn vẹn và tính xác thực của thông điệp.

Trường này có thể được chèn thêm nếu cần thiết để đảm bảo tổng chiều dài của AH là bội số của 32 bits (đối với Ipv4) và 64 bits (đối với Ipv6).

**3.3. Vị trí của AH**

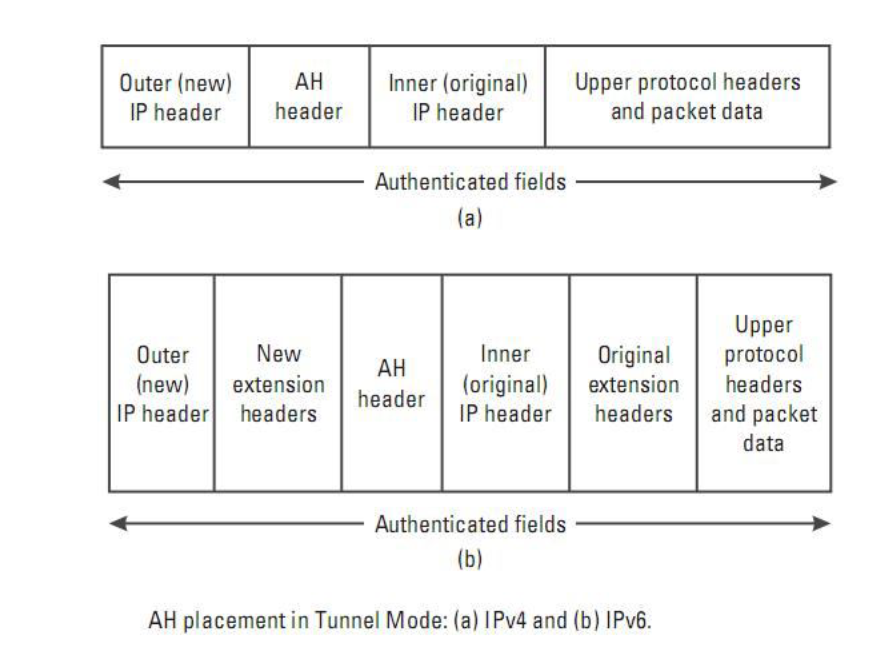
****

**Hình trên mô tả vị trí của tiêu đề AH trong các gói tin Ipv4 và Ipv6.**

Trong Ipv4, AH theo sau tiêu đề của gói tin Ip, tiếp đến là các tiêu đề của các giao thức ở trên (TCP, UDP, ICMP) hoặc tiêu đề ESP.

Trong Ipv6, vị trí của AH cũng tương tự như trên, tuy nhiên trong Ipv6 có thêm các tiêu đề tùy chọn. Vị trí tương quan của các tiêu đề này và AH như sau: Các tiêu đề của các tùy chọn mở rộng trong Ipv6 đứng trước AH là các tiêu đề hop-by-hop, tiêu đề định tuyến (routing header), tiêu đề phân mảnh (fragment header); Tiêu đề đích tùy chọn (dest options header) có thể đứng trước hoặc theo sau AH. Vị trí tương quan của tiêu đề này với AH phụ thuộc vào việc quá trình xử lí xác định đối với nó diễn ra trước hay sau khi quá trình xác thực diễn ra.

**3.4. Các mode làm việc trong AH**

****

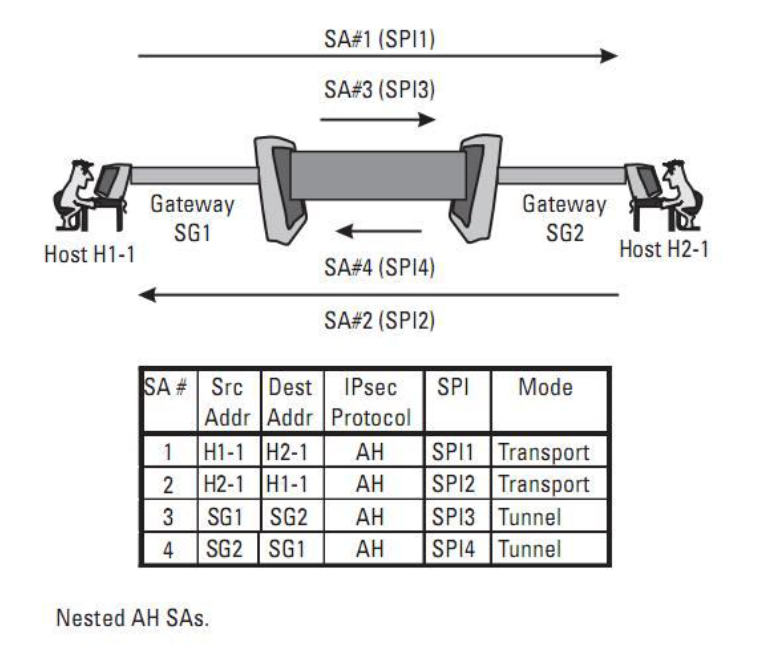
Hình trước minh họa vị trí của AH trong chế độ Transport, chế độ này thường được sử dụng để xác thực đầu cuối giữa hai host. Tuy nhiên trong trường hợp hai SG (security gateway) được sử dụng để bảo vệ cho nhiều host trong một mạng thì chế độ tunnel được sử dụng. Hình trên mô tả vị trí của AH trong chế độ tunnel. Chế độ tunnel cũng có thể sử dụng trong truyền thông giữa hai host trong trường hợp này địa chỉ trong tiêu đề ip ban đầu và tiêu đề ip bổ sung là như nhau.

**3.5. Nested và Adjacent header trong AH**

Nhiều SA có thể áp dụng cho một thông điệp. Nếu một trong hai đầu cuối của các thông điệp này là giống nhau thì các AH của các SA này được gọi là Adjacent AH. Nếu một hoặc hai đầu cuối của các SA khác nhau thì các AH này được gọi là các AH lồng (nested AH).

Adjacent AH không cung cấp thêm bất cứ sự bảo vệ nào cả, việc áp dụng chúng là không bắt buộc (not mandated).

Nested AH có thể được áp dụng trong một số trường hợp nhất định.

****

Hình trên minh họa việc một trường hợp sử dụng nested AHs. Trong ví dụ này: Host 1 và host 2 yêu cầu xác thực đầu cuối. Tuy nhiên các gateway của mỗi host này lại yêu cầu xác thực tất cả các gói tin qua gateway. Trong tình huống này nested AHs được sử dụng để thỏa mãn yêu cầu trên.

**3.6. Quá trình xử lý tiêu đề của IPSec**

Thông thường cơ chế xử lí đối với thông điệp trong mạng như sau: Đối với các thông điệp đi ra (Outbound messages), tiêu đề ip được thêm vào các thông điệp, sau đó chúng có thể được phân mành nếu cần. Tiếp theo chúng được chuyển xuống các tầng dưới và đi ra ngoài. Đối với các thông điệp đi vào, các thông điệp sẽ được giải phân mành nếu cần thiết, sau đó bỏ phần tiêu đề ip rồi chuyển lên các lớp trên để xử lí.

Khi sử dụng IPSEC thì các cơ chế xử lí trên cần có sự biến đổi. Có ba hướng tiếp cận để giải quyết vấn đề này:

Thay đổi cấu trúc mạng (IP stack code). Đây là cách tiếp cận trực tiếp nhất. Tuy nhiên điều này dẫn tới phải thay đổi ở trong lớp nhân (kernel code). Do đó nó thường áp dụng đối với các nhà phát triển hệ thống. Nó có thể áp dụng cho cả các host và gateways.

Thay đổi cấu trúc mạng (IP stack code). Đây là cách tiếp cận trực tiếp nhất. Tuy nhiên điều này dẫn tới phải thay đổi ở trong lớp nhân (kernel code). Do đó nó thường áp dụng đối với các nhà phát triển hệ thống. Nó có thể áp dụng cho cả các host và gateways.

Tách cấu trúc ip ra khỏi cấu mạng. Cách làm này không cần thay đổi cấu trúc của nhân. Tuy nhiên nó kéo theo việc phải thay đổi lại các cơ chế phân mảnh và giải phân mành. Cách làm này thường được gọi là “Bump in the stack" (BITS) bởi vì gói ipsec năm giữa tầng internet và tầng network của mô hình mạng. Cách này thường áp dụng cho cả host và gateway. Tuy nhiên nó thường được áp dụng đối với các host trong một hệ điều hành cũ. (legacy operating systems)

Đặt IPSEC ra ngoài hệ thống, cách làm này gọi là “Bump in the wire" (BITW). Trong cách làm này IPSEC có thể được tích hợp trong router hay firewall và được đặt trong router hoặc firewall, hoặc nó có thể đứng độc lập trong một IPSEC box. Nó có thể được gắn cho một host gateway hoặc một máy đa năng.

**3.7. Quá trình xử lí của AH đối với các gói tin Outbound:**

Một khi đã xác định rằng thông điệp gửi đi (outbound message) được bảo vệ bởi AH, và đã xác định được một SA phù hợp quản lí việc truyền thông điệp này. Thông điệp được chuyển tới quá trình xử lí IPSEC. Quá trình này gồm các bước như sau:

1. Thêm một khuôn dạng AH vào vị trí thích hợp.

2. Thêm vào trường next header.

3. Thêm vào trường SPI bằng giá trị SPI của SA được chọn ở trên.

4. Tính giá trị sequence number (giá trị max của trường này là 2^32 -1). Nếu giá trị này chưa đạt giá trị max thì chỉ cần tăng sequence number lên một đơn vị. Giá trị mới này được cất vào AH và SAD. Ngược lại khi sequence number đã đạt đến giá trị max thì có thể xáy ra các tình huống như sau: Nếu khóa bí mật giữa các bên của SA đã được thỏa thuận, đây là thời điểm thỏa thuận một khóa mới bất kể bên nhận có sử dụng chức năng chống phát lại hay không. Thông điệp này có thể được giữ lại hoặc hủy bỏ cho đến khi quá trình thỏa thuận khóa mới diễn ra. Nếu khóa của SA được tạo ra thủ công, nghĩa là hai bên thỏa thuận khóa với nhau thông qua một số cách xác định như là qua điện thoại hoặc sử dụng thư và nếu bên gửi biết rằng bên nhận không sử dụng chức năng chống phát lại thì sequence number đơn giản được reset về giá trị một. Đối với việc thỏa thuận khóa thủ công, trong trường hợp người nhận sử dụng chức năng chống phát lại, cần phải thỏa thuận một khóa mới. Cho tới lúc đó thông điệp chưa được gửi đi và quá trình xử lí AH lúc này bị treo (halt).

5. Đối với chế độ transport, trường next header được chuyển thành AH.

6. Thêm trường tiêu đề tunnel nếu cần thiết. Nếu SA sử dụng chế độ tunnel thì một tiêu đề ip bổ sung được tạo ra và thêm vào thông điệp. Địa chỉ nguồn và đích của tiêu đề ip bổ sung này là các đầu cuối của tunnel được xác định bởi SA.

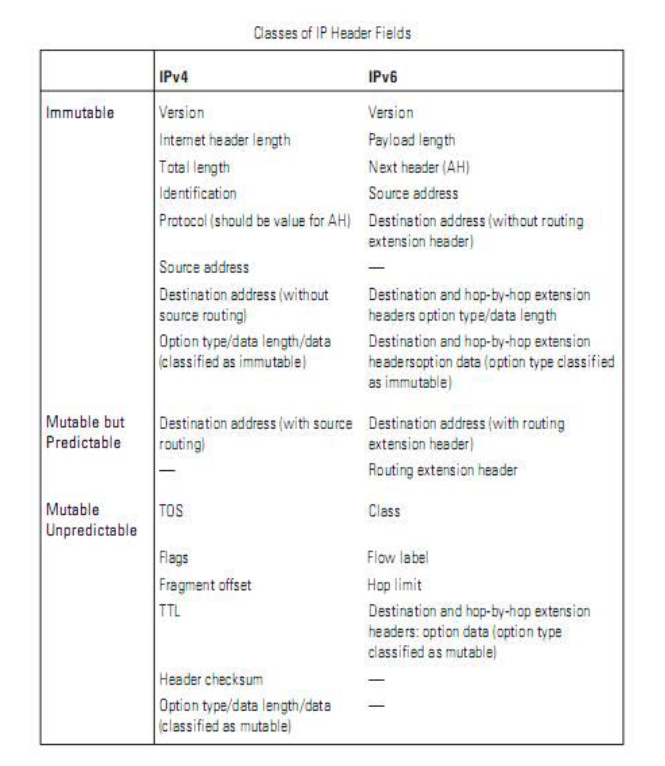
Nếu cả tiêu đề bên trong và bên ngoài đều là Ipv4 thì một số trường sau được chép từ inner header ra outer header: Version, TOS, Protocol, Fragment identification, MF Flag và Fragment offset. Một số trường sau cần phải tính toán lại: Header length, total length, và header checksum. Việc tính toán lại các giá trị này là cần thiết vì các trường này thể hiện cho cả outer header và inner header lẫn AH. Trường next header được thiết lập là AH. Trường optional không được sao chép. Trường TTL được thiết lập giá trị mặc định của hệ thống. Giá trị của cờ DF (don't fragment) tùy thuộc vào các policy của hệ thống cục bộ. Giá trị này có thể được chép từ inner header hoặc được gán giá trị bằng 1 để chống phân mành hoặc gán giá trị bằng 0 để cho phép phân mảnh. Các trường của inner header được giữ nguyên ngoại trừ một ngoại lệ: Nếu địa chỉ nguồn của inner header và outer header là khác nhau có nghĩa là gói tin bên trong đã đi đến địa điểm nguồn của tunnel do đó giá trị TTL (Time to live) bị giảm và do đó cần phải tính lại giá trị checksum trong inner header để phản ánh sự thay đổi này.

Nếu cả hai tiêu đề đều là Ipv6, một số trường sau được chép từ inner header ra outer header: Version và Traffic class. Trường Payload length được tính toán lại do tại thời điểm này trường này thể hiện giá trị tổng cộng của inner header outer header và AH. Trường next header được thiết lập là AH hoặc là giá trị của phần mở rộng tùy chọn đứng trước AH. Những trường mở rộng này không thể sao chép một cách thuần túy. Trường Hop limited được gán giá trị mặc định của hệ thống. Các trường của inner header được giữ nguyên ngoại trừ một ngoại lệ nếu địa chỉ nguồn của inner header và outer header khác nhau tức là gói tin inner đã đi đến địa điểm nguồn của tunnel. Lúc này giá trị Hop-limmited bị giảm đi một đơn vị. Điều này dẫn tới việc phải tính toán và cập nhật lại giá trị của trường checksum trong inner header.

Nếu inner header là Ipv4 header và outer header là Ipv6 header hoặc ngược lại thì quá trình xử lí có vài điểm khác biệt. Trường version field được thiết lập là 4 đối với Ipv4 header và 6 đối với Ipv6 header. Trường Traffic class được chuyển sang TOS, địa chỉ nguồn và địa chỉ đích được chuyển đổi sang định dạng phù hợp nếu cần thiết.

7. Tính toán dữ liệu xác thực. Lưu ý rằng toàn bộ thông điệp không được bảo vệ bởi AH, bởi vì ip header chứa 3 loại dữ liệu cơ bản sau: Immutable data (các dữ liệu không thay đổi trong quá trình truyền), mutable data but predicable (các dữ liệu thay đổi trong quá trình truyền nhưng có thể dự đoán được) và mutable unpredicable data (các dữ liệu thay đổi trong quá trình truyền và không thể dự đoán trước được). Bảng dưới đây sẽ phân loại các trường này trong Ipv4 header và Ipv6 header. Chi những trường chứa immutable data hoặc mutable data but predicable được đưa vào hàm băm để tính. Trong transport mode chỉ những trường này của ip header được đưa vào hàm băm. Trong tunnel mode toàn bộ inner header và thông điệp gốc được đưa vào hàm băm tuy nhiên chỉ những immutable data và mutable data but predicable của outer header được đưa vào hàm băm. Đối với các trường chứa dữ liệu mutable unpredic data có các hướng giải quyết như sau. Không đưa chúng vào hàm băm hoặc thay thế chúng bằng các giá trị zero. Trên thực tế người ta áp dụng cách thứ 2. Vì cách làm này đảm bảo hàm băm luôn thực hiện trên dữ liệu có chiều dài xác định, đây là cách làm tổng quát.

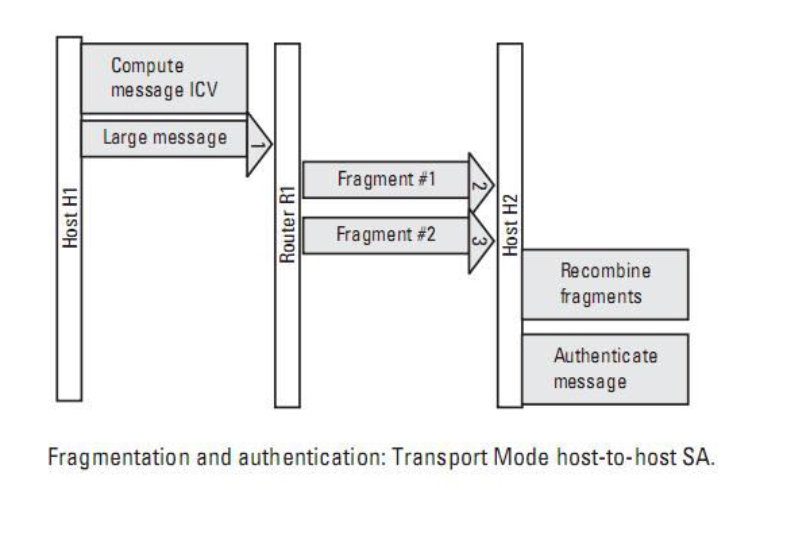
Thuật toán băm áp dụng với AH là HMAC-MD5 (sinh ra 128 bits) và HMAC-SHA1 (sinh ra 160 bits). Trong AH để đảm bảo cho số lượng byte ngoài biên được phù hợp cho quá trình xử lí AH giảm số lượng bits xuống còn 96 bits. Một khi đã thêm trường ICV vào AH thông điệp đã sẵn sàng

****

8. Phân mành thông điệp nếu cần thiết. Nếu việc thêm AH và đặc biệt thêm các tiêu đề trong tunnel mode làm kích thước thông điệp quá lớn thì việc phân mành là cần thiết. Việc phân mảnh có thể diễn ra tại thời điểm này.

Trong transport mode địa chỉ nguồn luôn luôn là địa chi khởi tạo của thông điệp nên toàn bộ thông điệp có thể xác thực trước khi quá trình phân mảnh diễn ra.

Trong tunnel mode địa chỉ nguồn của inner header luôn là địa chỉ khởi tạo của thông điệp, nếu địa chỉ này khác địa chỉ source của outer header thì thông điệp có thể đã bị phân mành trước khi rời khỏi host ban đầu. Trong trường hợp đó tunnle header xác thực trên thông điệp đã bị phân mành và có thể sẽ bị phân mành tại thời điểm này.

****

****

**3.8. Quá trình xử lí của AH đối với các gói tin Inbound:**

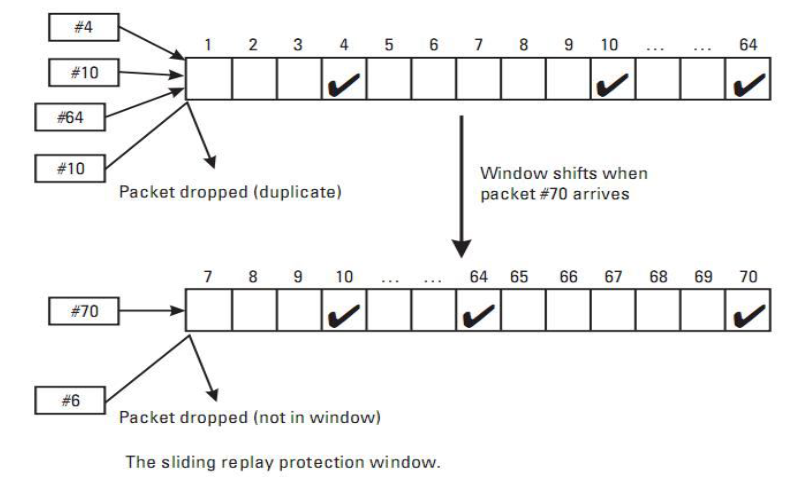
Khi nhận được một thông điệp có chứa AH, quá trình xử lí ip trước tiên sẽ tổng hợp các phân mành thành thông điệp hoàn chỉnh. Sau đó thông điệp này sẽ được chuyển tới quá trình xử lí IPSEC. Quá trình này gồm các bước như sau:

1. Xác định inbound SA tương ứng trong SAD. Bước này được thực hiện dựa trên các thông số: 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.

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.

3. Đối với mỗi inbound SA, SAD lưu trữ một cửa sổ chống phát lại. Kích thước của cửa số 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 cửừa số phát lại đều bị hủy bỏ. Các thông điệp có số sequence number đã tồn tại trong cửa số phát lại cũng bị hủy bỏ.

4. 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 số chống phát lại. hình dưới đây minh họa hoạt động của cửa sổ chống phát lại.

****

5. Kiểm tra tính xác thực của dữ liệu. Hàm băm được tính toán tương tự như outbound message. 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.

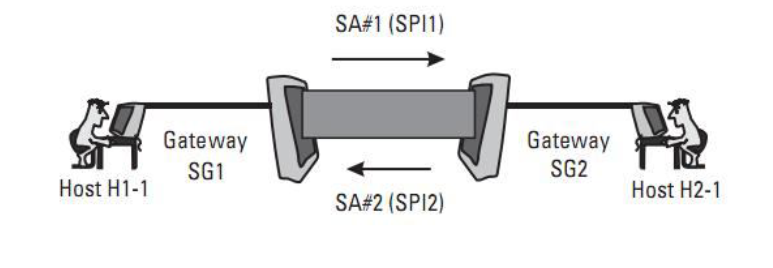
6. Loại bỏ AH và tiếp tục quá trình xử lí IPSEC cho các phần còn lại của tiêu đề IPSEC. Nếu có một nested IPSEC header xuất hiện tại đích đến này. Mỗi header cần phải được xử lí cho đến khi một trong hai điều kiện được thỏa mãn. Khi ipsec header cuối cùng đã được xử lí thành công và quá trình xử lí tiếp 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.

7. 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.

**3.9. Một số điểm phức tạp trong giao thức AH**

**3.9.1. Vấn đề phân mãnh và việc quản lý các gói ICMP trong giao thức AH**

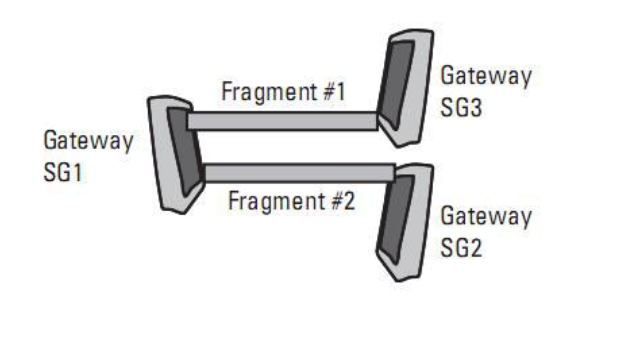
Hai vấn đề sau trong giao thức ip làm cho giao thức AH trở nên phức tạp: Quá trình phân mành và các thông điệp ICMP lỗi. Chúng ta sẽ tìm hiểu vấn đề này thông qua các ví dụ sau:

****

Xét ví dụ sau: Giả sử tunnel mode được thiết lập SG1 và SG2 để bảo vệ truyền thông giữa hai mạng N1 và N2. Nếu một gói tin từ H1 đến H2 đã được phân mảnh trước khi nó đến SG1(ta gọi đây là trường hợp 1) (việc này có thể được thực hiện bởi một router trung gian (trong Ipv4) hoặc host xuất phát (trong Ipv6), SG1 sẽ tính các giá trị ICV cho từng phân mảnh. Khi các phân mành này đến SG2 từng phân mảnh được xác thực riêng biệt trước khi chúng được giải phân mành. Gói tin sau khi đã được giải phân mảnh và được xác thực được chuyển tiếp đến đích đến H2. Tiếp theo ta giả sử tình huống sau quá trình phân mảnh được thực hiện tại một router nằm giữa SG1 và SG2 (chỉ xét trong Ipv4) (ta gọi đây là trường hợp 2). SG1 đã tính ICV cho toàn bộ gói tin. Khi các phân mành đến SG2 chúng cần phải được tổng hợp lại trước khi xác thực vì ICV đã được tính trước khi việc phân mảnh diễn ra.

Ta thay đổi tình huống như sau. Giả sử SG1 biết một số đoạn (segment) của đường truyền gặp vấn đề nghẽn cổ chai về kích thước gói. Do đó SG1 quyết định không thực thi tunnel mode trong AH để tránh việc thêm outer header nhằm làm giảm kích thước gói tin. Cách giải quyết này không phù hợp với kiến trúc của giao thức ipsec vì nó đã loại bỏ một số thành phân trong ipsec mà cụ thể là (tunnle mode).

Ta tiếp tục thay đổi mô hình mạng như sau:



Giả sử ngoài SG2, còn có SG3 phục vụ N2, được minh họa như hình vẽ trên. Nếu SA giữa N1 và N2 tất cả đều là tunnel mode SA, được thỏa thuận giữa SG1 và SG2 thì tất cả các gói phân mảnh sẽ được định tuyết qua các gateway thích hợp và thông điệp sẽ được xử lí một cách chính xác. Tuy nhiên nếu SG1 và SG2 quyết định giảm kích thước các gói tin và thiết lập transport mode SA thì vấn đề sẽ xuất hiện. SG2 thiết lập transport mode SA với giả định rằng nó là ngõ vào duy nhất với N2 do đó nó có thể bắt được tất cả các gói tin và thực hiện xác thực trước khi các gói tin đến H2. Nếu bất kì một gói tin nào được định tuyến thông qua SG3 thì quá trình tổng hợp sẽ diễn ra không chính xác.

Trường hợp 1, SG2 xác thực mỗi gói tin nó nhận được và cố gắng tổng hợp chúng lại. Tuy nhiên vì không phải tất cả các phân mảnh đều đi qua SG2, nên gói tin đang tổng hợp dỡ sẽ bị hủy bỏ khi thời gian tổng hợp hết (reasembly timer expires). Cùng lúc đó phân mảnh đến SG3 có thể bị SG3 hủy bỏ hoặc chuyển tiếp đến H2, tại đây không xác định được SA phù hợp cho phân mành trên nên nó bị hủy bỏ. Trong trường hợp 2, SG2 cố gắng tông hợp các gói tin trước khi xác thực chúng. Tuy nhiên kết quả vẫn diễn ra tương tự như trường hợp 1. Đây là trường hợp xấu nhất. Nhưng trên thực tế tình huống này lại xảy ra với tần suất đáng báo động. Minh họa trên lý giải vì sao phải áp dụng tunnel mode giữa hai gateway.

Để chống quá trình phân mành, các gateway cần phải thông báo với các host mà nó bào vệ về kích thước header mà nó có thể thêm vào gói được gửi bởi host đó. Host ban đầu thường cố gắng gửi các gói tin có kích thước xấp xỉ PMTU (path maximum tranmisstion unit). Chỉ cần trừ đi kích thước header mà các security gateway phải thêm vào thì quá trình phân mảnh có thể tránh được.

Ngoài ra còn có một cách tránh việc phân mảnh. Host ban đầu có thể kiểm tra mô hình mạng để xác định giá trị PMTU và dựa vào đó để điều chỉnh kích thước gói tin cho phù hợp. Kĩ thuật này trong Ipv4 đòi hỏi host source phải bật bit DF (Don't fragment) lên một, để tránh việc phân mảnh tại các router trung gian. Cách làm này có thể làm xuất hiện vấn đề khi áp dụng đối với IPSEC. Nếu một gói tin có kích thước quá lớn không thể đi qua toàn bộ các route, khi đó một router trung gian sẽ gửi một ICMP với thông điệp là “gói tin quá lớn” đến host ban đầu. Trong trường hợp tunnel mode SA, gói ICMP sẽ được gửi đến cho security gateway có địa chỉ là điạ chỉ source trong outer header. Vấn đề rất nghiêm trọng đặt ra là khi gói tin ICMP trên không phải được gửi từ đích đến cuối cùng của thông điệp mà là từ một router trung gian. Điều này lại càng nghiêm trọng khi áp dụng IPSEC vì trong ipsec các gói tin đều phải xác thực rõ nguồn gốc. Gateway sau khi nhận được gói tin trên sẽ phải lựa chọn giữa các phương án: Liệu có thể tin tưởng thông điệp trong gói ICMP chưa xác thực trên hay không? Nếu tin tưởng thì phải chuyển tiếp gói tin ICMP trên cùng với số PMTU mới đến host nguồn ban đầu (trong inner header). Nếu gateway không chuyển tiếp gói tin ICMP trên về host nguồn thì một lỗ hồng lớn sẽ xuất hiện: Host nguồn tiếp tục gửi các gói tin với cờ DF được bật lên vì nó không bao giờ nhận được gói tin thông báo về số PMTU mới, do đó nó không giảm kích thước của gói tin. Do đó các gói tin cứ tiếp tục được gửi đi làm tăng truyền thông trên mạng một cách vô ích vì chúng không bao giờ đến được đích cuối cùng.

Việc sử dụng các gói tin ICMP để gửi thông điệp về PMTU có thể bị lợi dụng để tấn công deny of service. Một attacker gửi một gói ICMP với một số PTMU nhỏ hơn giá trị PMTU cần thiết. Nếu gateway chấp nhận gói tin ICMP chưa được xác thực này và chuyển tiếp cho host ban đầu. Host ban đầu sẽ giàm kích thước cho tất cả các gói tin lưu thông trên con đường đó. Điều này dẫn tới việc gia tăng số lượng của các gói tin có kích thước nhỏ hơn đồng nghĩa với việc gia chi phí tính toán với các vấn đề IP liên quan, có thể làm gia tăng lưu lượng trên mạng và làm giảm chất lượng dịch vụ.

Một số giải pháp đưa ra đê khắc phục vân để đưa ra về PMTU. Giải pháp đầu tiên đòi hỏi sự hợp tác giữa SG1 và SG2.SG1 cho phép các gói tin đã phân mành từ H1 tiếp tục con đường của chúng. Để làm được điều này nếu innner header set bit DF thì outer header không set bit này. Khi SG2 nhận được các gói tin đã bị phân mành. Nó gửi một số PMTU đến SG1, thông báo cho SG1 biết về kích thước của phân mành lớn nhất đi qua đoạn đường từ SG1 đến SG2 thành công. Bởi vì đoạn đường từ SG1 đến SG2 đã thiết lập các cơ chế bảo vệ gói tin. Gói tin PMTU này khác so với các gói tin PMTU thông thường vì PMTU được gửi sau khi đã nhận các phân mảnh. Trong khi bình thường, gói PMTU là kết quả của việc truyền không thành công một phân mảnh. Một cách khác SG2 có thể lưu trữ PMTU như một thành phần của SA và đều đặn thông báo SG1 giá trị PMTU mới nhất. Nếu H1 cố gắng gửi một gói tin có kích thước quá lớn, SG1 sẽ thông báo giá trị PMTU hiện tại với H1. Cho đến thời điểm này chưa có thêm giải pháp nào cho vấn đề này được đưa ra.

**3.9.2. Mối quan hệ giữa NAT Và IPSec**

NAT là một kỹ thuật mạng cho phép nhiều thiết bị sử dụng một địa chỉ IP công cộng duy nhất để kết nối với Internet. Điều này giúp tiết kiệm địa chỉ IP công cộng và đơn giản hóa cấu hình mạng.NAT hoạt động bằng cách thay đổi địa chỉ IP nguồn và đích của các gói tin khi chúng đi qua một router.

**IPSec** là một tập hợp các giao thức bảo mật mạng được thiết kế để bảo vệ các giao tiếp IP**.** Nó cung cấp các dịch vụ như:

**Mã hóa:** Bảo vệ dữ liệu khỏi bị xem trộm.

**Xác thực:** Đảm bảo tính toàn vẹn của dữ liệu và xác nhận danh tính của các bên tham gia.

**Bảo mật:** Ngăn chặn các cuộc tấn công như giả mạo, từ chối dịch vụ.

**IPSec sử dụng hai giao thức chính:**

**AH (Authenticated Header):** Cung cấp xác thực và bảo vệ chống lại các cuộc tấn công replay.

**ESP (Encapsulating Security Payload):** Cung cấp mã hóa và xác thực.

### **Mối quan hệ giữa NAT và IPSec**

Mặc dù NAT và IPSec có chức năng khác nhau, nhưng chúng thường được sử dụng cùng nhau trong các mạng hiện đại. Dưới đây là một số lý do:

**NAT giúp bảo vệ mạng nội bộ:** Bằng cách ẩn các địa chỉ IP nội bộ, NAT giúp ngăn chặn các cuộc tấn công trực tiếp vào các máy chủ bên trong mạng.

**IPSec bảo vệ lưu lượng mạng:** IPSec cung cấp một lớp bảo mật bổ sung cho các gói tin đi qua NAT, đảm bảo rằng dữ liệu được truyền đi một cách an toàn và đáng tin cậy.

**NAT-T:** Để giải quyết vấn đề tương thích giữa NAT và IPSec, một giao thức mở rộng gọi là NAT-T (NAT Traversal) đã được phát triển. NAT-T cho phép các gói tin IPSec đi qua các thiết bị NAT mà không bị chặn.

### **Các vấn đề khi kết hợp NAT và IPSec:**

**NAT có thể làm thay đổi các trường trong tiêu đề IP**: Điều này có thể gây ra các vấn đề với các giao thức bảo mật như AH, vì AH dựa vào các trường trong tiêu đề IP để xác thực.

**NAT-T có thể gây ra độ trễ:** Việc đóng gói và giải gói các gói tin IPSec trong NAT-T có thể làm tăng độ trễ của kết nối.

**Cấu hình phức tạp:** Việc cấu hình NAT và IPSec đòi hỏi kiến thức chuyên sâu và có thể phức tạp, đặc biệt khi kết hợp chúng lại với nhau.

### **Kết luận**

NAT và IPSec là hai công nghệ bổ sung cho nhau, giúp bảo vệ mạng và dữ liệu một cách hiệu quả. Bằng cách hiểu rõ mối quan hệ giữa hai công nghệ này, bạn có thể thiết kế và triển khai các giải pháp bảo mật mạng phù hợp với nhu cầu của mình.

**3.9.3. Vấn đề auditing (giám sát) trong AH**

Trong AH (Authentication Header) của giao thức IPsec, auditing (giám sát) đóng một vai trò quan trọng trong việc theo dõi và kiểm tra các hoạt động bảo mật. Việc giám sát này đảm bảo rằng các giao thức bảo mật được triển khai và tuân thủ đúng cách, đồng thời phát hiện và ngăn chặn các hành vi trái phép, giúp nâng cao tính bảo mật và hiệu quả của hệ thống.

**Dưới đây là một số vấn đề liên quan đến auditing (giám sát) trong AH:**

**1. Giám sát hoạt động bảo mật (Security Activity Monitoring):**

**Mục tiêu:** Giám sát các hoạt động của hệ thống và người dùng để phát hiện các hành động đáng ngờ hoặc vi phạm bảo mật.

**Vấn đề:** Trong AH, một số loại thông tin quan trọng như mã xác thực (authentication) có thể không được ghi lại chi tiết, dẫn đến việc khó phát hiện các hành vi xâm nhập hoặc sự thay đổi không hợp lệ trong quá trình truyền tải.

**Giải pháp:** Việc giám sát nên bao gồm ghi lại tất cả các hành động bảo mật liên quan đến AH, chẳng hạn như các thay đổi về thông tin xác thực, việc sử dụng các khóa xác thực và các kết nối được bảo vệ.

**2. Theo dõi và kiểm tra tính toàn vẹn (Integrity Monitoring):**

**Mục tiêu:** Đảm bảo rằng dữ liệu không bị thay đổi hoặc bị xâm nhập trong quá trình truyền tải.

**Vấn đề:** Mặc dù AH cung cấp bảo vệ tính toàn vẹn của gói tin, nhưng việc theo dõi các hành vi có thể làm thay đổi hoặc giả mạo dữ liệu (ví dụ: tấn công replay, tấn công vào các thông số giao thức) lại không được kiểm soát thường xuyên.

**Giải pháp:** Giám sát các giao thức bảo mật AH giúp phát hiện các thay đổi hoặc thay thế gói tin, đồng thời yêu cầu phải kiểm tra và xác thực toàn bộ chuỗi giao dịch bảo mật.

**3. Giám sát các thay đổi trong cấu hình (Configuration Changes):**

**Mục tiêu:** Kiểm soát các thay đổi trong cấu hình của AH hoặc các thành phần khác trong giao thức IPsec.

**Vấn đề:** Việc thay đổi cấu hình, ví dụ như thay đổi các khóa xác thực, có thể dẫn đến các vấn đề về bảo mật nếu không được theo dõi chặt chẽ.

**Giải pháp:** Việc giám sát này yêu cầu có các công cụ theo dõi các thay đổi cấu hình, đồng thời cung cấp cảnh báo kịp thời khi có sự thay đổi quan trọng trong môi trường bảo mật.

**4. Giám sát và báo cáo sự cố bảo mật (Security Incident Reporting):**

**Mục tiêu:** Ghi nhận và báo cáo các sự cố liên quan đến bảo mật, giúp các quản trị viên có thể phản ứng kịp thời.

**Vấn đề:** Một số sự cố bảo mật có thể không được ghi nhận đầy đủ hoặc không được xử lý kịp thời, làm giảm hiệu quả của AH trong việc ngăn chặn tấn công.

**Giải pháp:** Giám sát phải bao gồm việc tạo và lưu trữ nhật ký các sự kiện bảo mật, cung cấp thông tin chi tiết về các cuộc tấn công hoặc xâm nhập vào hệ thống để phân tích và khôi phục dữ liệu.

**5. Quản lý và bảo vệ dữ liệu log (Log Data Management and Protection):**

**Mục tiêu:** Đảm bảo rằng các dữ liệu log ghi lại từ quá trình giám sát được bảo vệ khỏi sự sửa đổi hoặc mất mát.

**Vấn đề:** Nếu các dữ liệu log của AH không được bảo vệ hoặc lưu trữ đúng cách, có thể bị xóa hoặc thay đổi, làm giảm tính hiệu quả của quá trình giám sát.

**Giải pháp:** Cần có cơ chế bảo mật mạnh mẽ để bảo vệ dữ liệu log, bao gồm việc mã hóa log, sao lưu định kỳ và kiểm soát truy cập đối với các file log.

**6. Giám sát hiệu suất và độ tin cậy (Performance and Reliability Monitoring):**

**Mục tiêu:** Giám sát hiệu suất của hệ thống AH, đảm bảo rằng các giao thức bảo mật hoạt động hiệu quả và không làm gián đoạn các dịch vụ mạng.

**Vấn đề:** Các giao thức bảo mật có thể gây ra độ trễ hoặc ảnh hưởng đến hiệu suất mạng, nhưng điều này không phải lúc nào cũng được giám sát thường xuyên.

**Giải pháp:** Các công cụ giám sát hiệu suất nên được triển khai để theo dõi các chỉ số mạng như độ trễ, băng thông và tải trọng hệ thống để đảm bảo rằng AH không làm suy giảm hiệu suất của toàn bộ hệ thống.

**7. Phân tích sự kiện bảo mật (Security Event Analysis):**

**Mục tiêu:** Phân tích các sự kiện bảo mật để phát hiện các mối đe dọa tiềm ẩn hoặc xác định nguyên nhân của sự cố.

**Vấn đề:** Phân tích các sự kiện bảo mật liên quan đến AH có thể khó khăn và mất thời gian, đặc biệt nếu không có đủ công cụ phân tích phù hợp.

**Giải pháp:** Các công cụ phân tích bảo mật nâng cao cần được sử dụng để theo dõi các sự kiện liên quan đến AH, giúp phát hiện các điểm yếu trong hệ thống bảo mật.

**Kết luận:**

Auditing (giám sát) trong giao thức AH là rất quan trọng trong việc đảm bảo rằng các giao thức bảo mật và các hoạt động mạng diễn ra an toàn và đáng tin cậy. Việc triển khai giám sát hiệu quả giúp phát hiện các sự cố bảo mật sớm, giảm thiểu các nguy cơ xâm nhập và vi phạm bảo mật. Tuy nhiên, để đạt được hiệu quả, quá trình giám sát cần phải được thiết kế toàn diện, liên tục cập nhật và tối ưu hóa để thích ứng với các mối đe dọa và yêu cầu bảo mật mới

**4. Giao thức ESP**

**4.1 ESP (Encapsulating Security Payload)**:

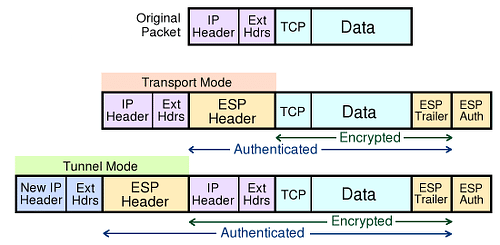
**ESP (Encapsulating Security Payload):** là một giao thức bảo mật quan trọng trong IPsec. Nó cung cấp một lớp bảo mật cho dữ liệu truyền đi qua mạng, bao gồm cả việc mã hóa, xác thực và bảo vệ tính toàn vẹn của dữ liệu.

**Các cơ chế bảo vệ chính của ESP:**

**1. Mã hóa (Encryption):**

**Bảo vệ bí mật:** Dữ liệu được mã hóa bằng các thuật toán mã hóa mạnh như AES, đảm bảo rằng chỉ những người có khóa giải mã mới có thể đọc được.

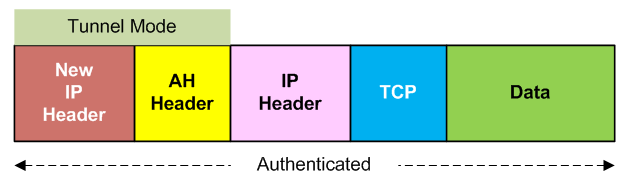
**Ngăn chặn nghe lén:** Ngăn chặn kẻ tấn công đọc được nội dung của gói tin khi chúng truyền đi trên mạng.

****

**2. Xác thực (Authentication):**

**Xác định nguồn gốc:** ESP sử dụng các hàm băm như SHA-1, SHA-256 để tạo ra một mã băm duy nhất cho dữ liệu. Mã băm này được đính kèm vào gói tin và được người nhận sử dụng để xác minh tính toàn vẹn của dữ liệu và xác định xem gói tin có bị thay đổi hay không.

**Ngăn chặn giả mạo:** Ngăn chặn kẻ tấn công thay đổi nội dung của gói tin mà không bị phát hiện.

****

**3. Bảo vệ tính toàn vẹn (Integrity):**

**Phát hiện thay đổi:** ESP đảm bảo rằng dữ liệu không bị thay đổi trong quá trình truyền đi. Nếu có bất kỳ thay đổi nào, mã băm sẽ không khớp và gói tin sẽ bị loại bỏ.

**4. Bảo mật kết nối (Confidentiality):**

**Tạo đường hầm ảo:** ESP tạo ra một đường hầm ảo an toàn để truyền dữ liệu giữa hai điểm cuối, đảm bảo rằng dữ liệu được truyền đi một cách riêng tư và bảo mật.

### **4.2 Cấu trúc của giao thức ESP:**

**Giao thức của ESP bao gồm các trường sau:**

**Security Parameters Index :** Một số nhận dạng duy nhất liên kết một gói tin với một Security Association cụ thể. SA xác định các tham số bảo mật như thuật toán mã hóa, thuật toán xác thực, khóa, v.v.

**Sequence Number:** Một số tuần tự tăng dần để ngăn chặn việc tái phát các gói tin và phát hiện các gói tin bị mất.

**Payload Data:** Dữ liệu thực tế của gói tin, bao gồm cả tiêu đề IP gốc và dữ liệu của lớp trên.

**Padding:** Một số lượng byte thêm vào để đảm bảo rằng kích thước của gói tin được bội số của một giá trị nhất định, thường là 8 byte. Điều này cần thiết cho một số thuật toán mã hóa.

**Authentication Data:** Một mã xác thực, được tính toán dựa trên tất cả các trường trước đó của tiêu đề ESP và dữ liệu tải trọng. Mã này được sử dụng để xác thực tính toàn vẹn của gói tin.

### **Chế độ hoạt động của ESP:**

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

**Transport Mode:** Trong chế độ này, chỉ dữ liệu của lớp trên được mã hóa và xác thực. Tiêu đề IP gốc vẫn ở dạng rõ. Chế độ này thường được sử dụng để bảo vệ các giao thức như TCP hoặc UDP.

**Tunnel Mode:** Trong chế độ này, toàn bộ gói IP gốc, bao gồm cả tiêu đề IP, được mã hóa và xác thực. Một tiêu đề IP mới sẽ được thêm vào bên ngoài để chứa tiêu đề ESP và dữ liệu đã mã hóa. Chế độ này thường được sử dụng để tạo các đường hầm VPN.

**Các chức năng chính của ESP:**

**Mã hóa:** Bảo vệ dữ liệu khỏi bị nghe trộm.

**Xác thực:** Đảm bảo tính toàn vẹn của dữ liệu và xác định nguồn gốc của gói tin.

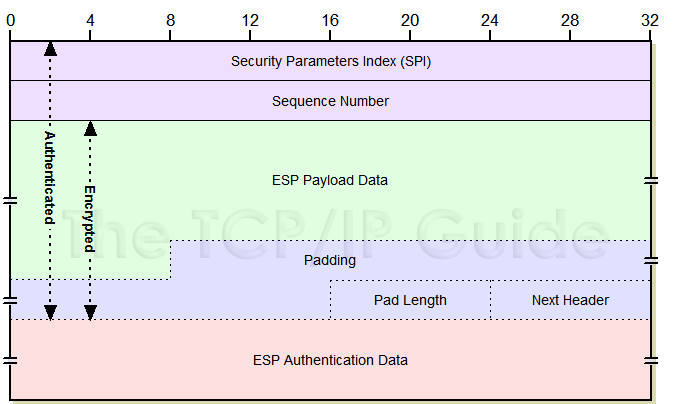
**Bảo mật:** Cung cấp một kênh truyền thông an toàn giữa các hệ thống.

### **Ưu điểm của ESP:**

**Linh hoạt:** ESP hỗ trợ nhiều thuật toán mã hóa và xác thực khác nhau.

**Hiệu quả:** ESP có thể được triển khai phần cứng để tăng tốc độ xử lý.

**Tiêu chuẩn:** ESP là một tiêu chuẩn mở, được hỗ trợ rộng rãi bởi các hệ điều hành và thiết bị mạng.



### **Ứng dụng của ESP:**

ESP được sử dụng rộng rãi trong các ứng dụng đòi hỏi bảo mật cao, như:

**VPN:** Tạo các đường hầm VPN an toàn để kết nối các mạng riêng qua Internet.

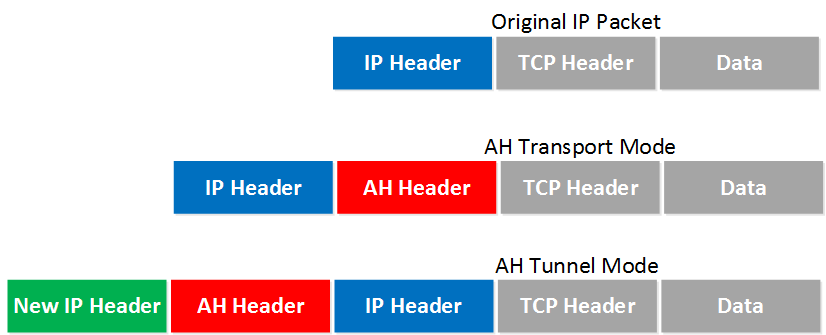
**IPsec:** Cung cấp bảo mật cho các giao thức IP.

**Wireless LAN:** Bảo vệ các mạng không dây.

**4.3. vị trí và các mode làm việc của giao thức ESP**

### Vị trí của ESP trong gói tin IP

Trong một gói tin IP sử dụng ESP, header ESP sẽ được chèn vào giữa header IP gốc và phần dữ liệu. Điều này có nghĩa là toàn bộ dữ liệu gốc, bao gồm cả header IP, sẽ được mã hóa và xác thực trước khi được truyền đi.



**Header IP:** Phần đầu của gói tin IP chứa thông tin định tuyến.

**ESP Header:** Phần đầu ESP chứa thông tin về bảo mật như SPI (Security Parameter Index), Sequence Number, và các thông tin xác thực.

**Payload:** Phần dữ liệu gốc được mã hóa và xác thực.

**Các chế độ làm việc của ESP:**

#### **1. Chế độ Tunnel (Đường hầm):**

**Mô tả:** Trong chế độ này, toàn bộ gói IP gốc, bao gồm cả header IP và dữ liệu, được gói vào một gói ESP mới. Gói ESP mới này lại được gói vào một gói IP mới với địa chỉ IP nguồn và đích mới.

**Ưu điểm:** Bảo vệ toàn bộ gói tin, bao gồm cả địa chỉ IP nguồn và đích, giúp ẩn danh các thiết bị trong mạng nội bộ.

**Sử dụng:** Thường được sử dụng để tạo các đường hầm VPN giữa các mạng riêng ảo.

#### **2. Chế độ Transport (Vận chuyển):**

**Mô tả:** Trong chế độ này, chỉ có phần dữ liệu (payload) của gói IP gốc được mã hóa và đóng gói vào một gói ESP. Header IP gốc vẫn được giữ nguyên.

**Ưu điểm:** Đơn giản hơn chế độ Tunnel và thường được sử dụng khi các thiết bị đầu cuối đã biết cách xử lý các gói IP có header ESP.

**Sử dụng:** Thường được sử dụng để bảo vệ các giao thức cấp cao như HTTP, FTP.

## **4.4 Nested và Adjacent Header trong Giao thức ESP:**

### **1. Nested Header:**

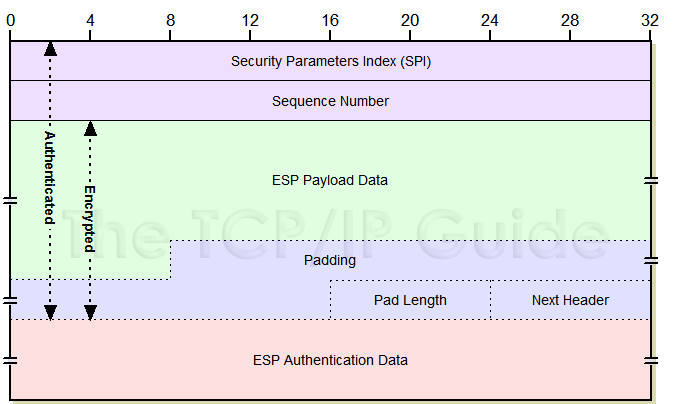
**Định nghĩa:** Nested Header là một tiêu đề ESP được nhúng bên trong một gói tin IP khác. Nó được sử dụng để bảo vệ một phần hoặc toàn bộ gói tin bên trong.

**Chức năng:**

**Bảo vệ dữ liệu:** Mã hóa và xác thực dữ liệu nhạy cảm bên trong gói tin.

**Tạo đường hầm:** Tạo một đường hầm ảo để truyền dữ liệu an toàn qua mạng không tin cậy.

**Vị trí:** Nested Header thường được đặt ở vị trí payload của gói tin IP bên ngoài.



### **2. Adjacent Header:**

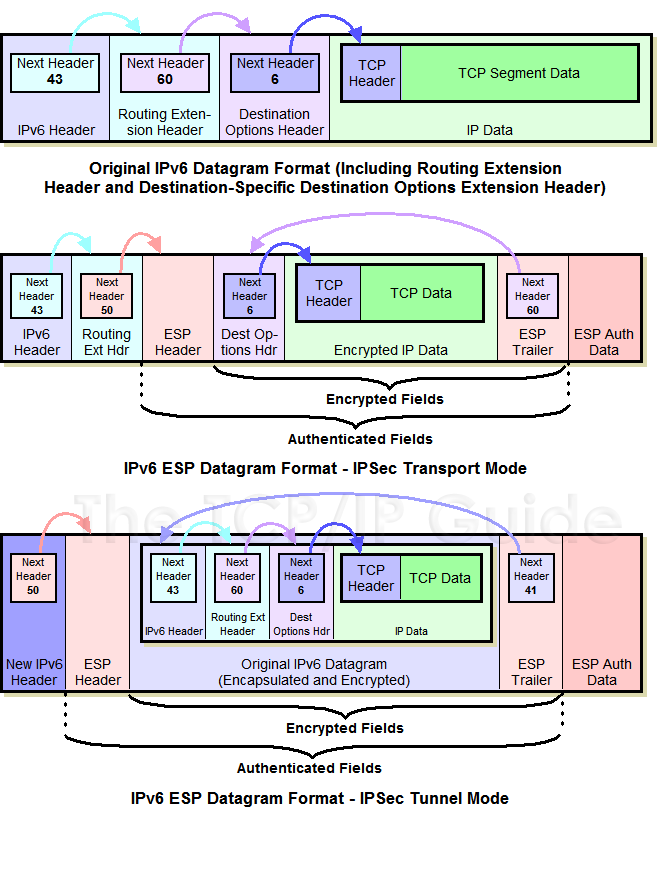
**Định nghĩa:** Adjacent Header là một tiêu đề ESP được đặt liền kề với tiêu đề IP của gói tin. Nó được sử dụng để bảo vệ toàn bộ gói tin IP, bao gồm cả tiêu đề và dữ liệu.

**Chức năng:**

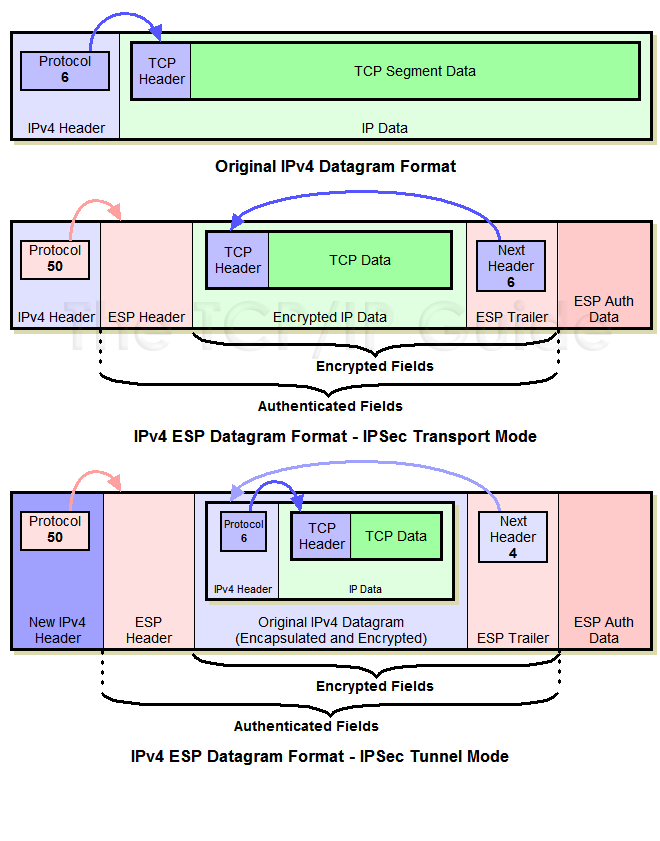
**Bảo vệ toàn bộ gói tin:** Mã hóa và xác thực cả tiêu đề IP và dữ liệu.

**Ngăn chặn phân tích lưu lượng:** Làm cho việc phân tích lưu lượng trở nên khó khăn hơn.

**Vị trí:** Adjacent Header thường được đặt ngay sau tiêu đề IP của gói tin.



**Định dạng Datagram IPv6 với IPsec Encapsulating Security Payload (ESP)**



**Định dạng Datagram IPv4 với IPsec Encapsulating Security Payload (ESP)**



**Ứng dụng của Nested và Adjacent Header**

**VPN:** Tạo các đường hầm VPN an toàn để kết nối các mạng riêng qua Internet.

**IPsec:** Cung cấp bảo mật cho các giao thức IP.

**Wireless LAN:** Bảo vệ các mạng không dây.

### **Lựa chọn giữa Nested và Adjacent Header:**

Việc lựa chọn giữa Nested Header và Adjacent Header phụ thuộc vào yêu cầu bảo mật cụ thể của mỗi ứng dụng.

**Nested Header:** Thích hợp cho các trường hợp cần bảo vệ một phần dữ liệu trong gói tin hoặc tạo các đường hầm VPN phức tạp.

**Adjacent Header:** Thích hợp cho các trường hợp cần bảo vệ toàn bộ gói tin và ngăn chặn việc phân tích lưu lượng.

**4.5. Quá trình xử lí của ESP đối với các gói tin Ounbound**

### **Quá trình xử lý gói tin outbound của ESP:**

### **1. Tạo Header ESP:**

**SPI (Security Parameter Index):** Một số nhận dạng duy nhất cho một kết nối bảo mật.

**Sequence number:** Số thứ tự của gói tin.

**Các trường khác:** Thông tin về thuật toán mã hóa, xác thực, và các thông tin khác liên quan đến SA (Security Association).

**2. Mã hóa dữ liệu:**

**Chọn thuật toán:** Dựa vào SA, ESP sẽ chọn thuật toán mã hóa phù hợp (ví dụ: AES, 3DES).

**Mã hóa:** Dữ liệu gốc (bao gồm cả header IP nếu ở chế độ Tunnel) sẽ được mã hóa bằng thuật toán đã chọn.

**3. Tính toán mã xác thực:**

**Chọn hàm băm:** Dựa vào SA, ESP sẽ chọn hàm băm phù hợp (ví dụ: SHA-1, SHA-256).

**Tính toán:** Tính toán mã băm của dữ liệu đã mã hóa và các thông tin khác trong header ESP.

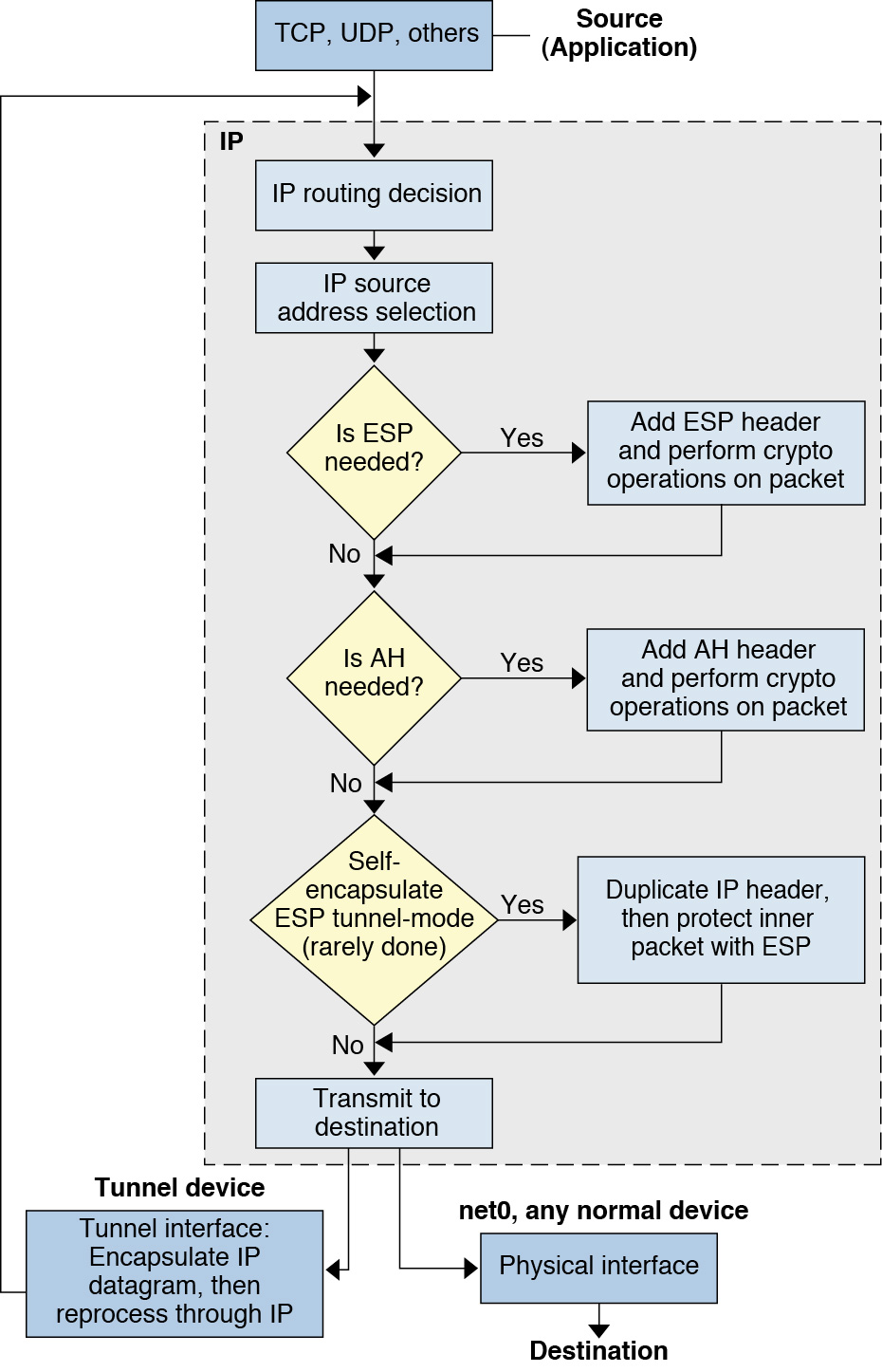
**Đính kèm:** Đính kèm mã băm vào cuối gói tin.

**4. Đóng gói:**

**Chế độ Tunnel:** Toàn bộ gói IP gốc được gói vào một gói ESP mới, sau đó gói ESP này lại được gói vào một gói IP mới với địa chỉ IP nguồn và đích mới.

**Chế độ Transport:** Chỉ phần dữ liệu của gói IP gốc được mã hóa và đóng gói vào một gói ESP. Header IP gốc vẫn được giữ nguyên.

**5. Gửi gói tin:**Gói tin đã được xử lý bởi ESP sẽ được gửi đi qua mạng.



### **Các thành phần chính trong quá trình xử lý:**

**SA (Security Association):** Một kết nối bảo mật được thiết lập giữa hai điểm cuối, xác định các thông số bảo mật như thuật toán mã hóa, xác thực, và các khóa.

**SPI:** Một số nhận dạng duy nhất cho một SA, giúp phân biệt các kết nối bảo mật khác nhau.

**Sequence number:** Giúp ngăn chặn các gói tin bị tái phát (replay attack).

**Integrity check value (ICV):** Mã băm dùng để xác minh tính toàn vẹn của dữ liệu.

### **Tổng kết**

Quá trình xử lý gói tin outbound của ESP đảm bảo rằng dữ liệu được truyền đi một cách an toàn và đáng tin cậy. Bằng cách mã hóa, xác thực và bảo vệ tính toàn vẹn của dữ liệu, ESP giúp ngăn chặn các cuộc tấn công như nghe lén, giả mạo, và thay đổi dữ liệu.

**4.6. Quá trình xử lý của ESP đối với gói tin Inbound**

Quá trình xử lý của ESP đối với gói tin inbound (gói tin đến máy nhận) bao gồm các bước sau:

**1.** **Xác thực tính toàn vẹn:** Gói tin sẽ được kiểm tra tính toàn vẹn bằng cách sử dụng mã xác thực.

**2. Giải mã dữ liệu:** Dữ liệu được giải mã nếu đã được mã hóa.

**3. Loại bỏ ESP trailer:** Phần trailer được loại bỏ, trong đó có padding và các thông tin hỗ trợ.

**4. Trả lại dữ liệu gốc:** Sau khi giải mã và kiểm tra tính toàn vẹn, dữ liệu gốc sẽ được trả lại cho ứng dụng hoặc hệ thống đích.

### **4.7. Một số điểm phức tạp trong giao thức ESP**

Một số vấn đề phức tạp trong giao thức ESP bao gồm:

**1. Quản lý khóa mã hóa:** Việc quản lý các khóa mã hóa và các thuật toán bảo mật phức tạp có thể gây khó khăn, đặc biệt trong môi trường lớn.

**2. Tăng chi phí và độ trễ:** Mã hóa và giải mã có thể tăng chi phí xử lý và độ trễ trong việc truyền tải dữ liệu.

**3. Phức tạp trong cấu hình và triển khai:** Để triển khai ESP một cách hiệu quả, cần có cấu hình chính xác và đồng bộ giữa các thiết bị mạng.

**4. Bảo mật trong môi trường lạ:** ESP có thể gặp khó khăn trong việc bảo vệ dữ liệu khi truyền qua các mạng không tin cậy, đặc biệt khi có sự thay đổi hoặc giả mạo trong gói tin.

### **4.8. Một số đánh giá, phê bình của các chuyên gia về ESP**

Một số chuyên gia chỉ ra rằng mặc dù ESP là một giao thức mạnh mẽ và có hiệu quả trong việc bảo vệ bảo mật và tính toàn vẹn của dữ liệu, nhưng có một số vấn đề cần cải thiện:

**1.** **Hiệu suất giảm:** Việc mã hóa và giải mã dữ liệu có thể ảnh hưởng đến hiệu suất mạng.

**2.** **Khó triển khai:** Cấu hình ESP trong môi trường doanh nghiệp có thể khó khăn và đắt đỏ.

**3.** **Phức tạp trong quản lý khóa:** Việc quản lý khóa mã hóa có thể gây phức tạp khi triển khai trong các mạng quy mô lớn

### **4.9. Lý do sử dụng hai tiêu đề bảo vệ**

**1.** **Phân tách chức năng:** Việc phân tách chức năng giữa AH và ESP giúp tăng cường tính linh hoạt và hiệu quả. AH tập trung vào xác thực và bảo vệ tính toàn vẹn, trong khi ESP tập trung vào mã hóa và bảo vệ bí mật.

**2. Tùy chọn cấu hình:** Người quản trị mạng có thể lựa chọn sử dụng AH, ESP hoặc cả hai tùy thuộc vào yêu cầu bảo mật của từng giao dịch.

**3. Quản lý khóa:** Việc quản lý khóa mã hóa là một trong những thách thức lớn nhất trong việc triển khai ESP. Cần có các cơ chế quản lý khóa an toàn và hiệu quả để đảm bảo tính bảo mật của hệ thống.

**4.** **Hiệu năng:** ESP có thể ảnh hưởng đến hiệu năng của mạng, đặc biệt là trong các môi trường có băng thông hạn chế.

Tương thích: ESP cần phải tương thích với các thiết bị mạng khác nhau và các giao thức mạng khác.

**Kết luận:**

ESP là một giao thức bảo mật mạnh mẽ và quan trọng trong việc bảo vệ dữ liệu truyền qua mạng. Tuy nhiên, việc triển khai và quản lý ESP đòi hỏi kiến thức chuyên sâu và sự cẩn trọng. Các chuyên gia cần cân nhắc kỹ lưỡng các yếu tố như hiệu năng, chi phí, và mức độ bảo mật khi lựa chọn và cấu hình ESP.

**II. Tìm hiểu về VPN**

**1. Khái niệm VPN:**

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

**2. Các mô hình triển khai:**

**2.1. VPN Site-to-Site (Mạng-tới-Mạng):**

**Mô tả:** Kết nối hai mạng riêng biệt (ví dụ: hai văn phòng của một công ty) qua internet, tạo thành một mạng thống nhất. Các máy tính trong mỗi mạng có thể truy cập tài nguyên của mạng kia một cách an toàn.

**Ứng dụng:** Kết nối các chi nhánh, cho phép nhân viên từ xa truy cập mạng nội bộ, kết nối các đối tác kinh doanh.

**Giao thức phổ biến:** IPSec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security).

**2.2. VPN Client-to-Site (Máy khách-tới-Mạng):**

**Mô tả:** Cho phép một thiết bị cá nhân (ví dụ: máy tính xách tay, điện thoại di động) kết nối an toàn vào một mạng từ xa (ví dụ: mạng công ty).

**Ứng dụng:** Nhân viên làm việc từ xa truy cập mạng công ty, người dùng truy cập mạng gia đình từ bên ngoài.

**Giao thức phổ biến:** PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec, OpenVPN, SSTP (Secure Socket Tunneling Protocol).

**2.3. VPN cá nhân (cho người dùng cá nhân):**

**Mô tả:** Dịch vụ VPN được cung cấp bởi một nhà cung cấp bên thứ ba, cho phép người dùng ẩn địa chỉ IP, mã hóa lưu lượng truy cập internet và truy cập nội dung bị chặn địa lý.

**Ứng dụng:** Bảo vệ quyền riêng tư trực tuyến, truy cập nội dung bị giới hạn khu vực, bảo mật khi sử dụng Wi-Fi công cộng.

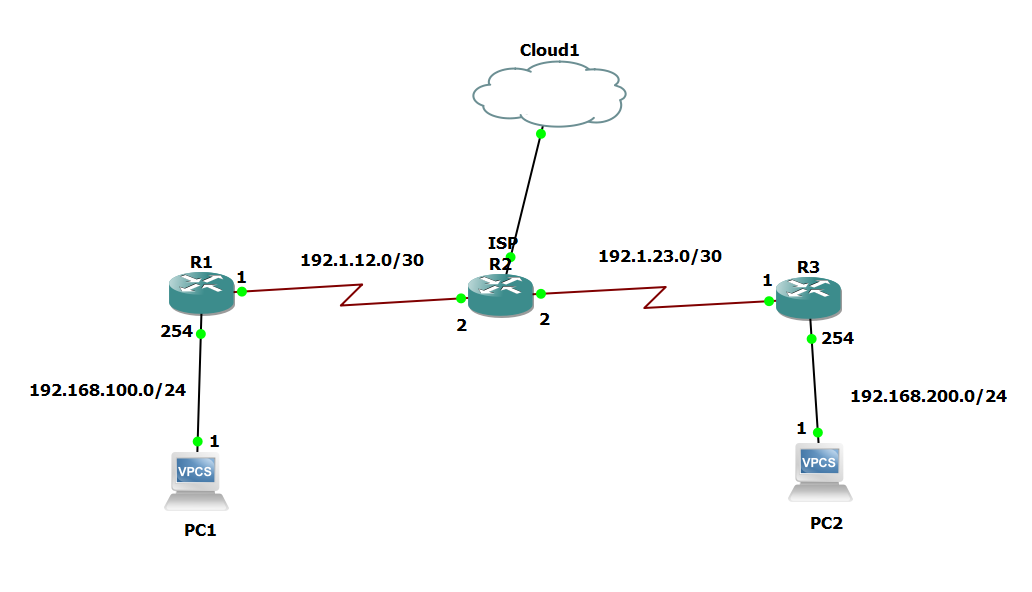
**Cách thức triển khai:**

* Sử dụng ứng dụng hoặc phần mềm VPN được cài đặt trên thiết bị.
* Sử dụng bộ định tuyến VPN.

**III. Triển khai hệ thống IPSec VPN trên phần mềm giả lập GNS3**

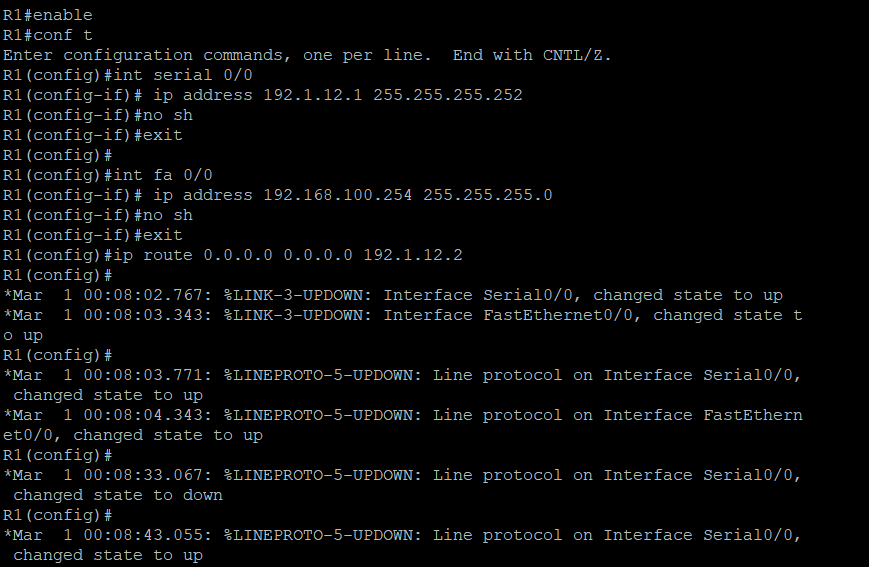
**1. Thiết lập mô hình Site-to-site**

**1.1. Thiết lập lab VPN IPSEC site to site:**

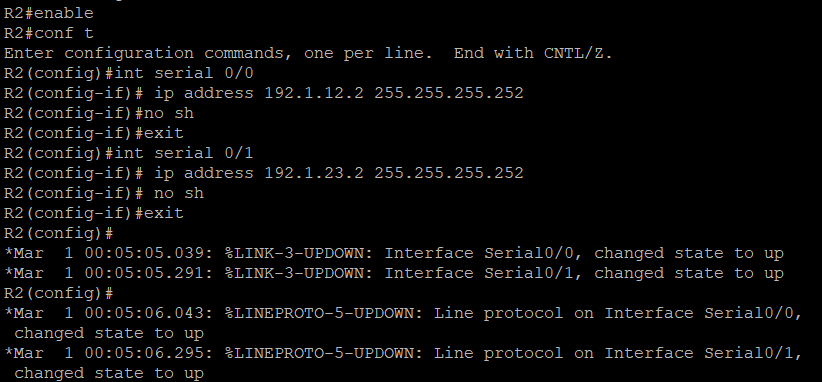
****

**Cấu hình gán IP và định tuyến tĩnh tại Router 1, Router 2, Router 3:**

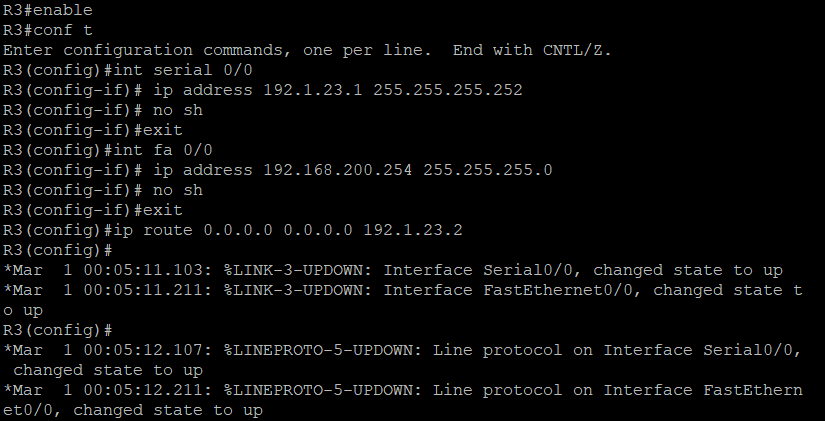
**Router 1:**

****

**Router 2:**

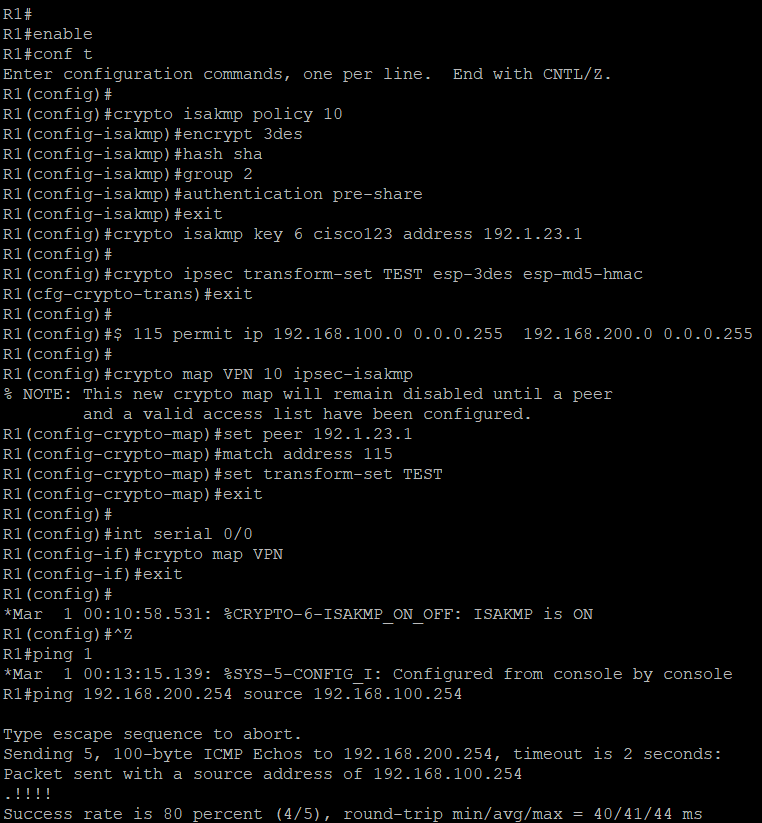
****

**Router 3:**

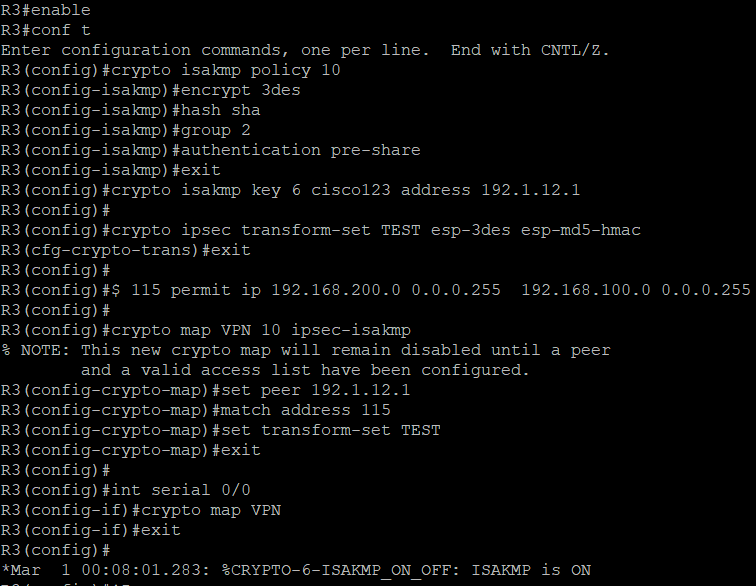
****

**1.2. Cấu hình VPN IPSEC site to site:**

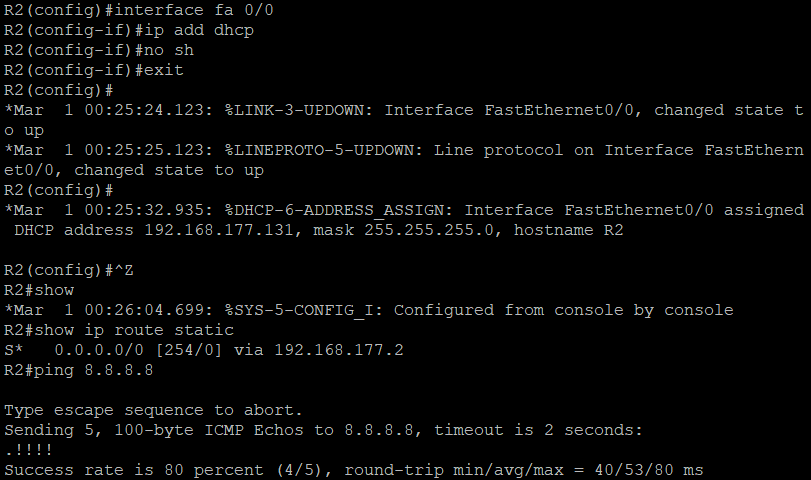
**Router 1:**

****

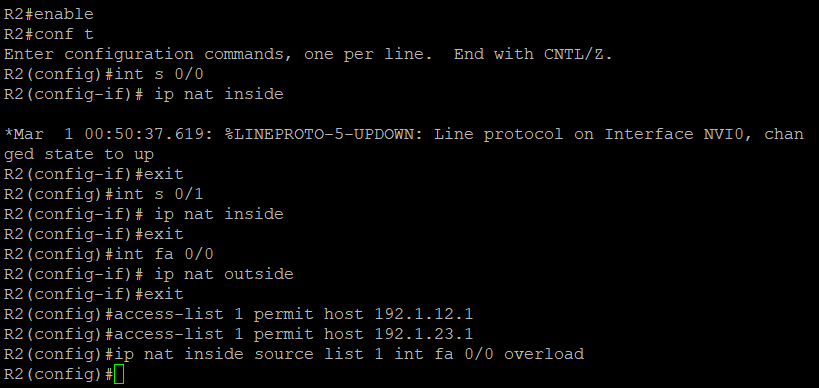
**Router 3:**

****

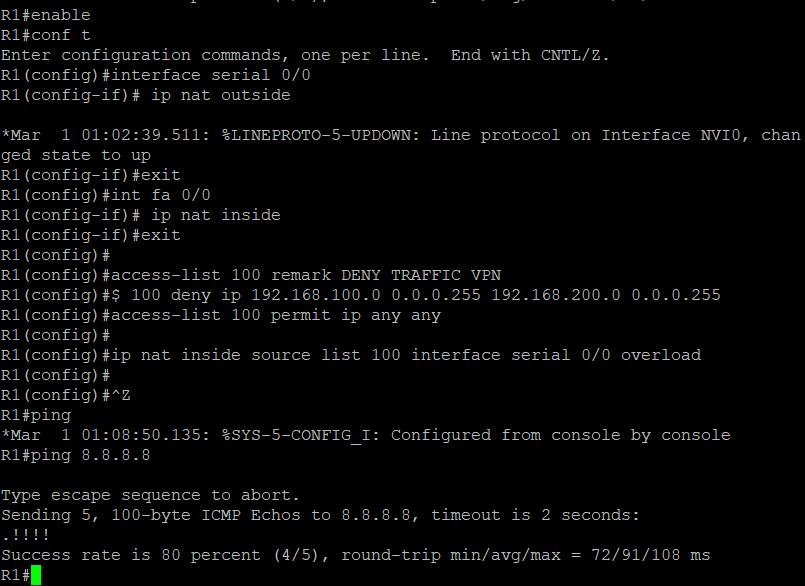
**1.3. Cấu hình DHCP với VMware Network Adapter VMnet8:**

****

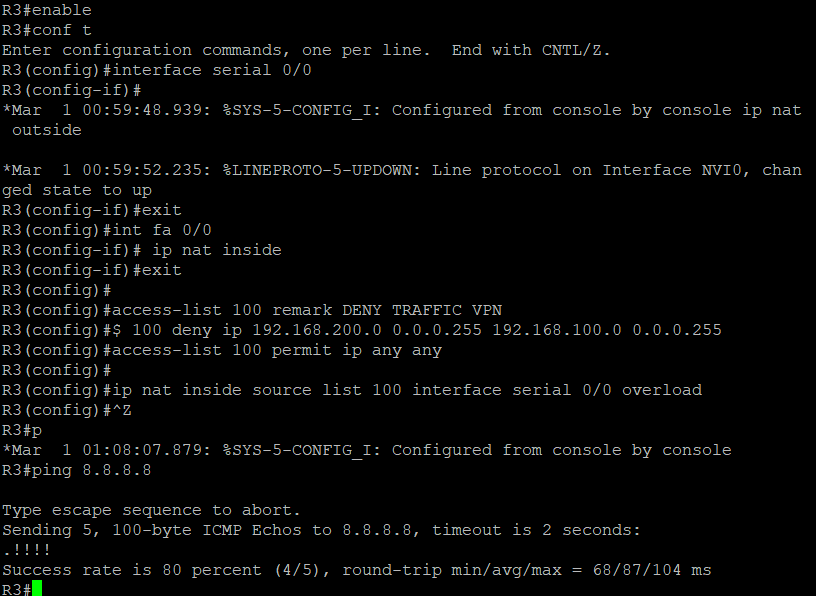
**1.4. Thiết lập NAT với VPN server:**

****

**1.4.1. Cấu hình Port address translation tại router 1:**

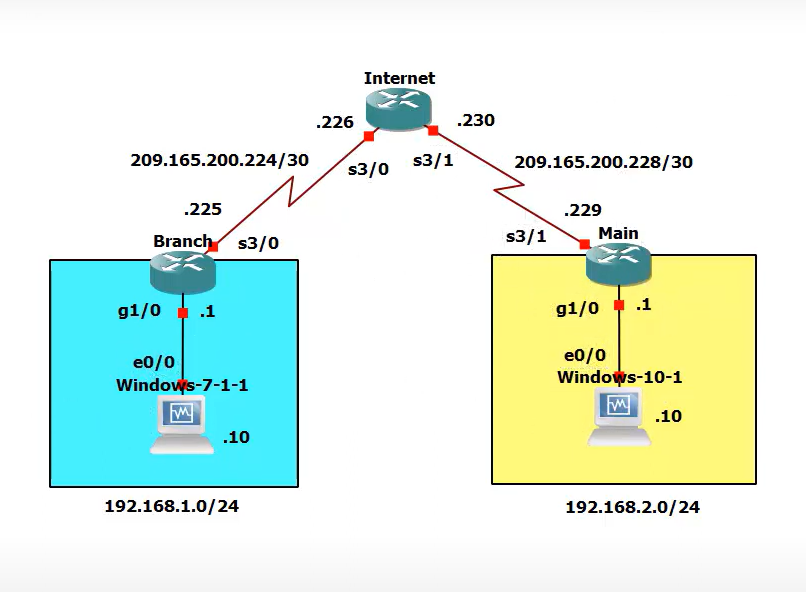
****

**1.4.2. Cấu hình Port address translation tại router 3:**

****

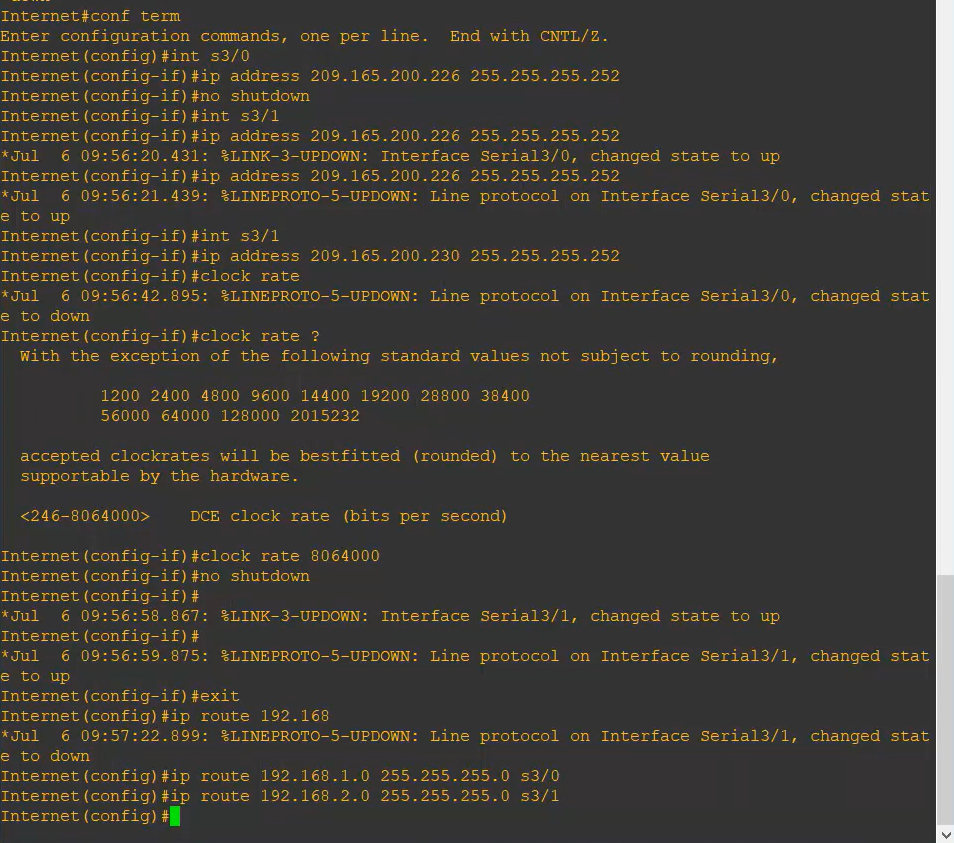
**2. Thiết lập theo mô hình Client-to-site (Remote access)**

* 1. **Thiết lập lab VPN IPSEC Client-to-site (Remote access)**

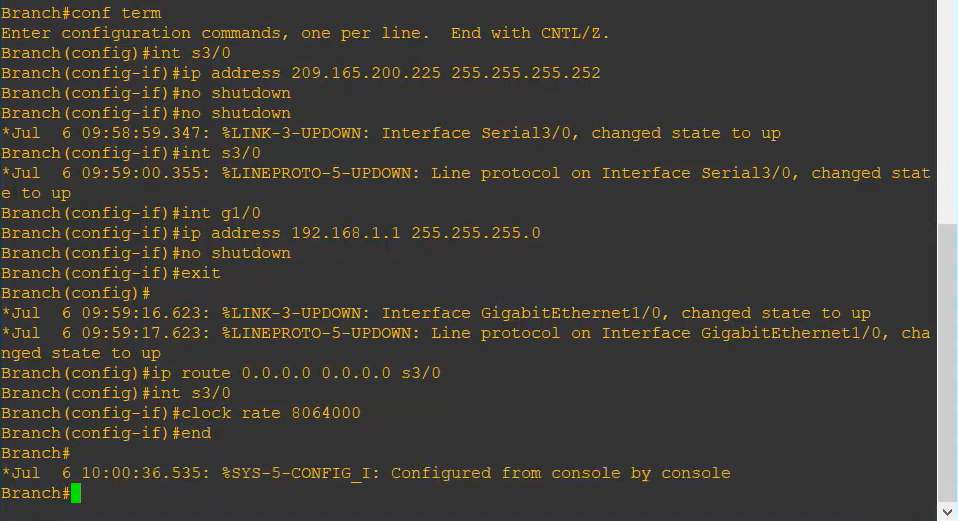


* 1. **Cấu hình router và gắn IP cho các router:**

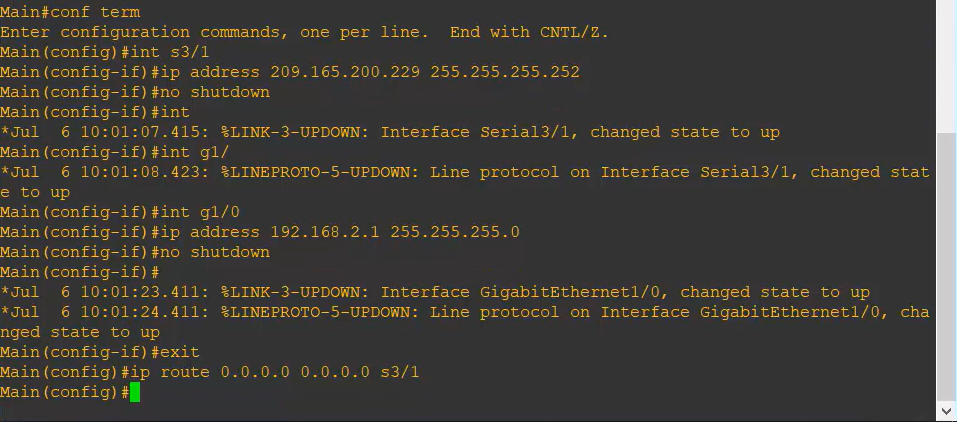
**Router Internet:**



**Router Branch (Router nhánh):**

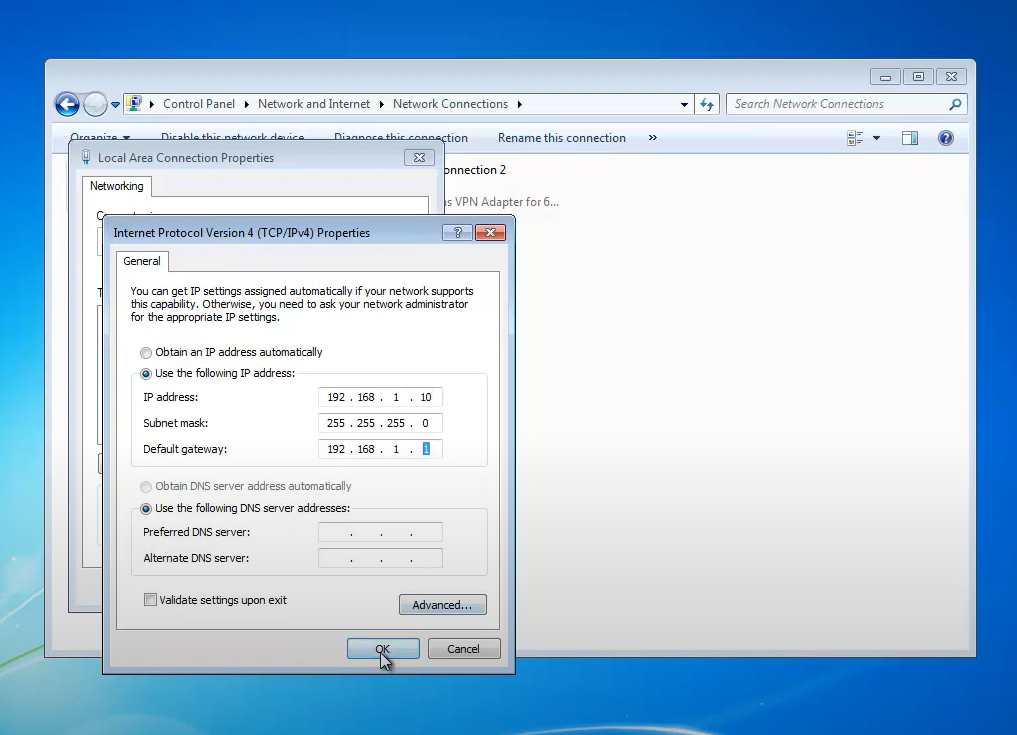


**Router Main (Router chính):**

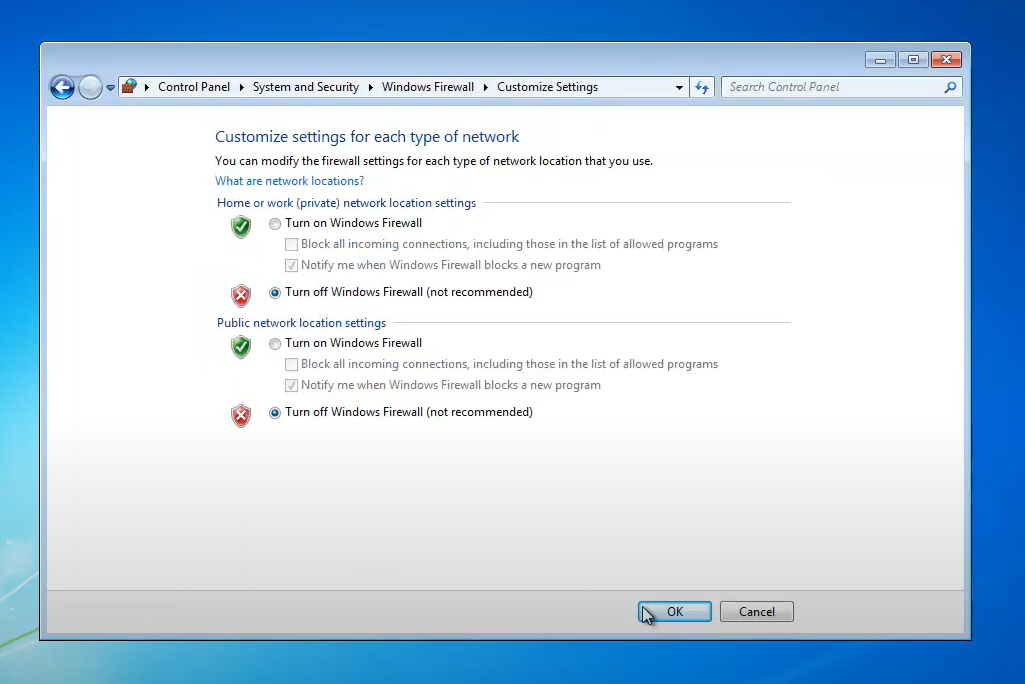


* 1. **Bật máy ảo tại GNS3 đã tích hợp với Oracle VM VirtualBox để đặt TCP/IPv4 và tắt Firewall (tường lửa).**

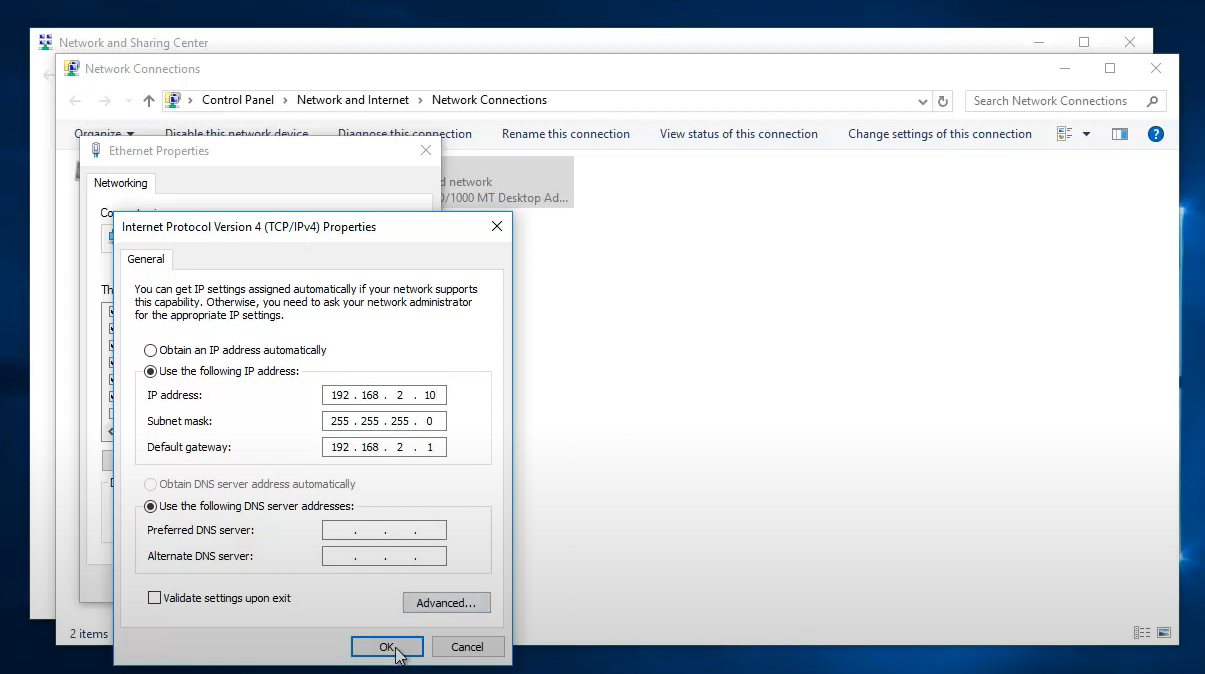
**Máy ảo Windows-7: IP address 192.168.1.10**



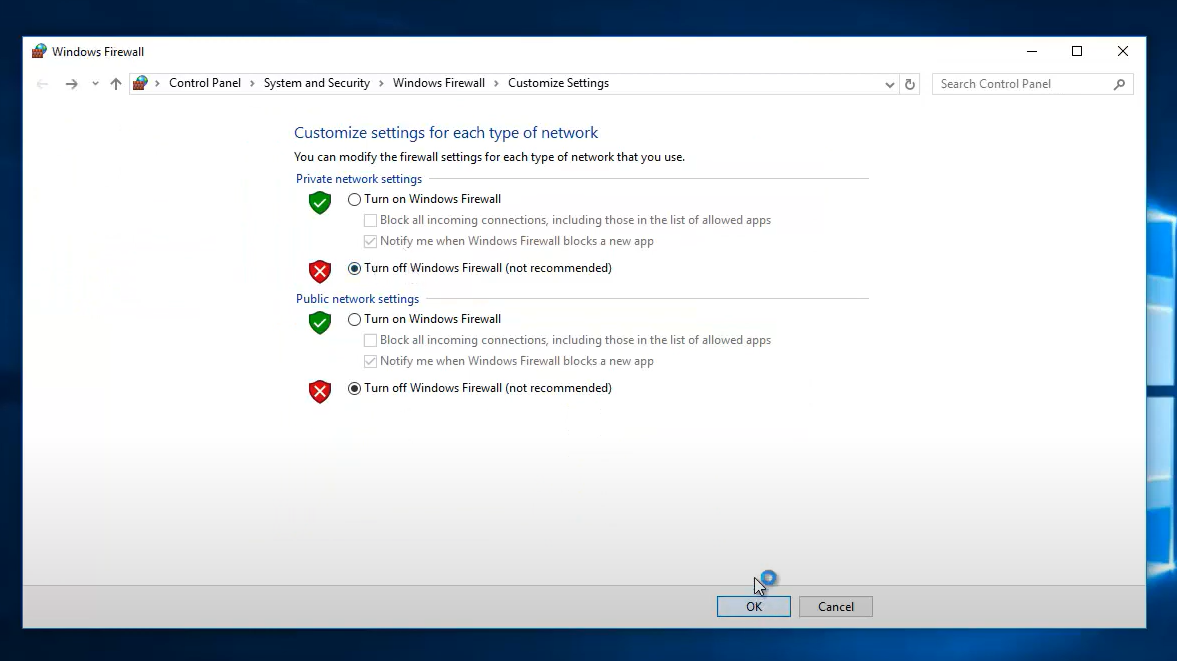
**Tắt Firewall (tường lửa) trên máy ảo Windows-7:**



**Máy ảo Windows-10: IP address 192.168.2.10**

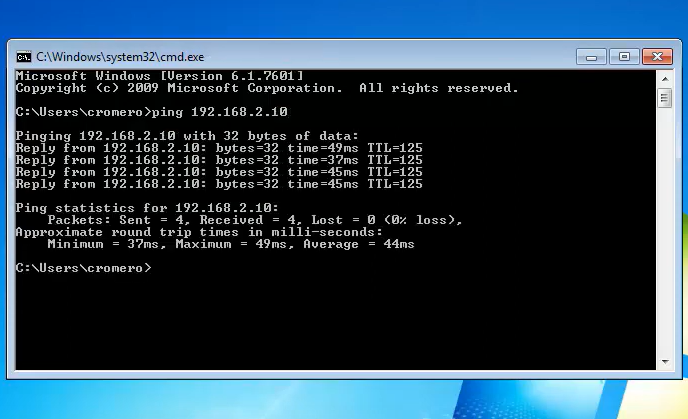


**Tắt Firewall (tường lửa) ở trên máy ảo Windows**-10:

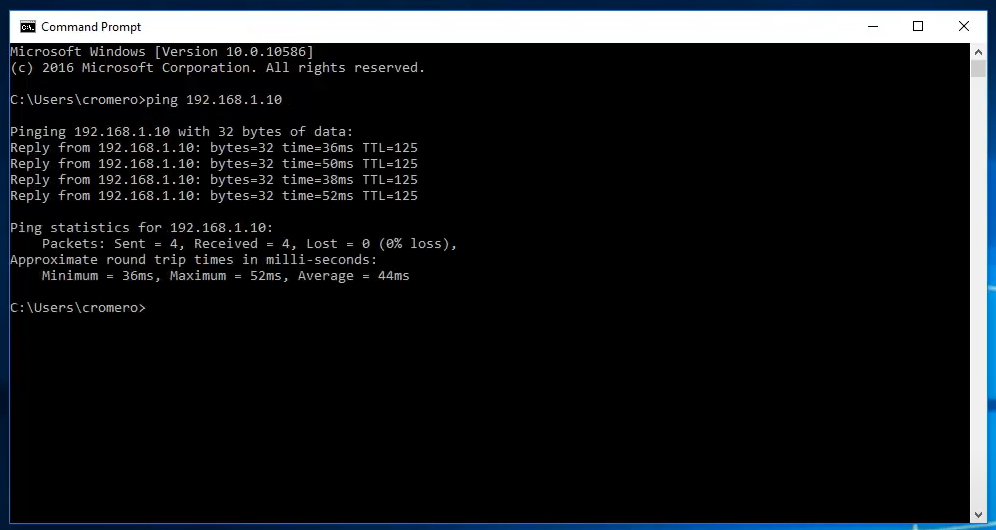


* 1. **Kiểm tra 2 máy ảo thông với nhau bằng Command Prompt.**

**Máy ảo Windows-7:**



**Máy ảo Windows-10:**



**IV. Tài Liệu Tham Khảo:**

1. [**https://luanvan.co/luan-van/ipsec-va-trien-khai-he-thong-ipsecvpn-tren-windows-server-2003-34959/?fbclid=IwZXh0bgNhZW0CMTAAAR10E9mhyH\_FPpKJ1C35scAPI7VwcjAEnyAI58nX9\_IFWVCPcuV6W3d1kFI\_aem\_Qqzr\_yqyG3r63VLeq2dwtg**](https://luanvan.co/luan-van/ipsec-va-trien-khai-he-thong-ipsecvpn-tren-windows-server-2003-34959/?fbclid=IwZXh0bgNhZW0CMTAAAR10E9mhyH_FPpKJ1C35scAPI7VwcjAEnyAI58nX9_IFWVCPcuV6W3d1kFI_aem_Qqzr_yqyG3r63VLeq2dwtg)
2. [**https://www.lecuong.info/2011/01/vpn-site-to-site-cisco.html**](https://www.lecuong.info/2011/01/vpn-site-to-site-cisco.html)
3. [**https://www.forum.vnpro.org/forum/ccnp-enterprise/sd-wan/30731-lab-vpn-site-to-site**](https://www.forum.vnpro.org/forum/ccnp-enterprise/sd-wan/30731-lab-vpn-site-to-site)