Chương 7

AN TOÀN IP

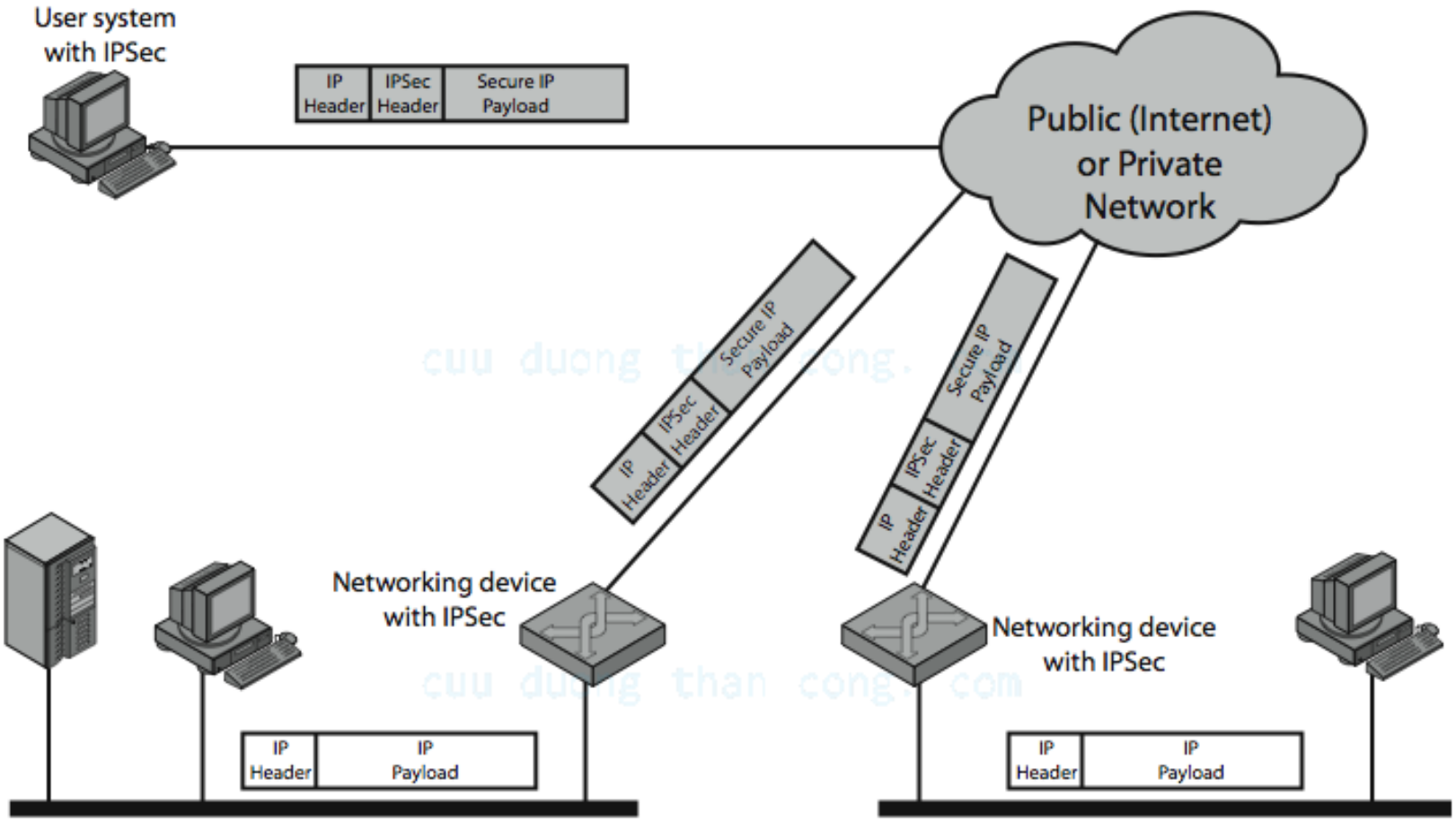
Giới thiệu

- Lý do cần IPSec
  - Có những vấn đề an ninh cần giải quyết ở mức thấp hơn tầng ứng dụng
    - Đặc biệt các hình thức tấn công ở tầng IP rất phổ biến như giả mạo IP, xem trộm gói tin
  - An ninh ở mức IP sẽ đảm bảo an ninh cho tất cả các ứng dụng
    - Bao gồm nhiều ứng dụng chưa có tính năng an ninh
- Các cơ chế an ninh của IPSec
  - Xác thực
  - Bảo mật
  - Quản lý khóa

Các ứng dụng của IPSec

- Xây dựng mạng riêng ảo an toàn trên Internet
  - Tiết kiệm chi phí thiết lập và quản lý mạng riêng
- Truy nhập từ xa an toàn thông qua Internet
  - Tiết kiệm chi phí đi lại
- Giao tiếp an toàn với các đối tác
  - Đảm bảo xác thực, bảo mật và cung cấp cơ chế trao đổi khóa
- Tăng cường an ninh thương mại điện tử
  - Hỗ trợ thêm cho các giao thức an ninh có sẵn của các ứng dụng Web và thương mại điện tử

Minh họa ứng dụng IPSec



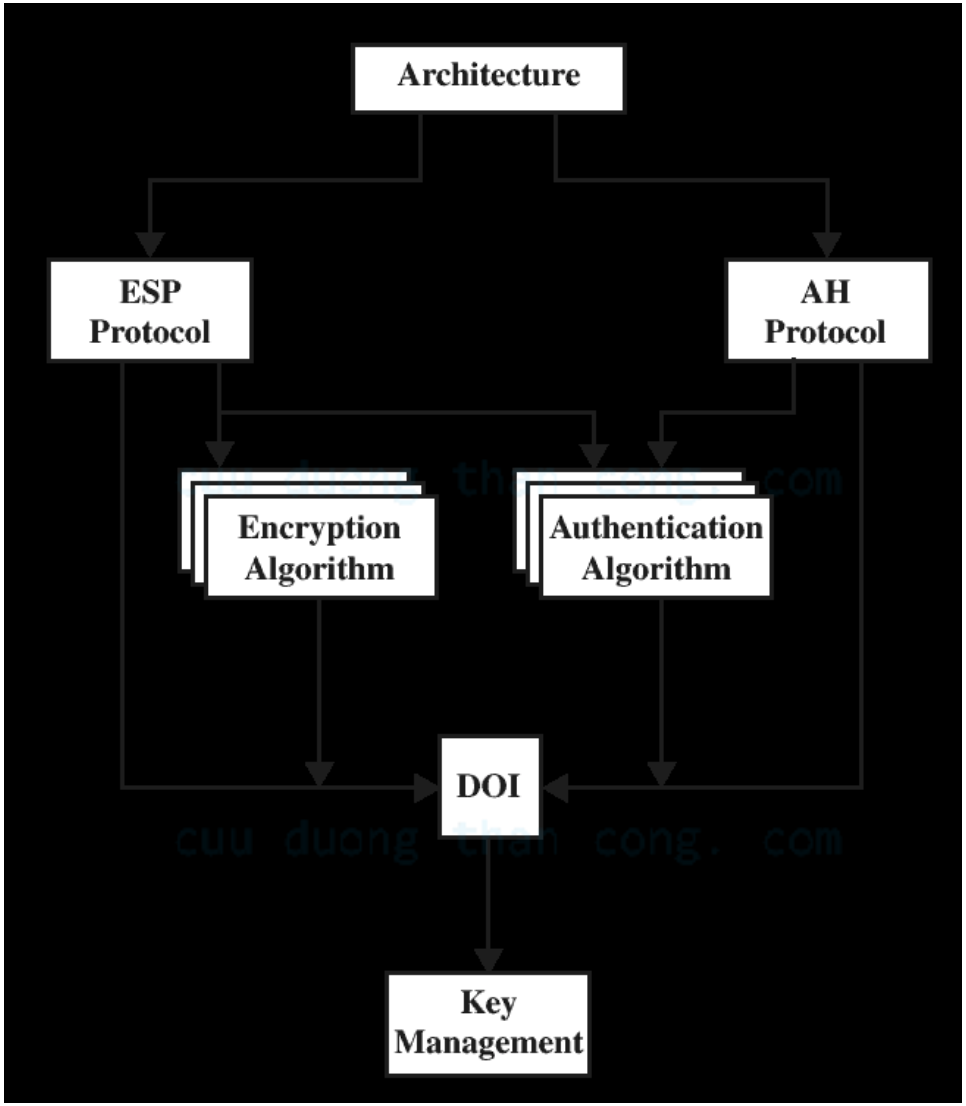
Ích lợi của IPSec

- Tại tường lửa hoặc bộ định tuyến, IPSec đảm bảo an ninh cho mọi luồng thông tin vượt biên
- Tại tường lửa, IPSec ngăn chặn thâm nhập trái phép từ Internet vào
- IPSec nằm dưới tầng giao vận, do vậy trong suốt với các ứng dụng
- IPSec có thể trong suốt với người dùng cuối
- IPSec có thể áp dụng cho người dùng đơn lẻ
- IPSec bảo vệ an ninh kiến trúc định tuyến

Kiến trúc an ninh IP

- Đặc tả IPSec khá phức tạp
- Định nghĩa trong nhiều tài liệu
  - Bao gồm RFC 2401 (tổng quan kiến trúc), RFC 2402 (mô tả mở rộng xác thực), RFC 2406 (mô tả mở rộng mã hóa), RFC 2408 (đặc tả khả năng trao đổi khóa)
  - Các tài liệu khác được chia thành 7 nhóm
- Việc hỗ trợ IPSec là bắt buộc đối với IPv6, tùy chọn đối với IPv4
- IPSec được cài đặt như các phần đầu mở rộng sau phần đầu IP
  - Phần đầu mở rộng cho xác thực là AH
  - Phần đầu mở rộng cho mã hóa là ESP

Tổng quan tài liệu IPSec



Các dịch vụ IPSec

- Bao gồm
  - Điều khiển truy nhập
  - Toàn vẹn phi kết nối
  - Xác thực nguồn gốc dữ liệu
  - Từ chối các gói tin lặp
    - Một hình thức của toàn vẹn thứ tự bộ phận
  - Bảo mật (mã hóa)
  - Bảo mật luồng tin hữu hạn
- Sử dụng một trong hai giao thức
  - Giao thức xác thực (ứng với AH)
  - Giao thức xác thực/mã hóa (ứng với ESP)

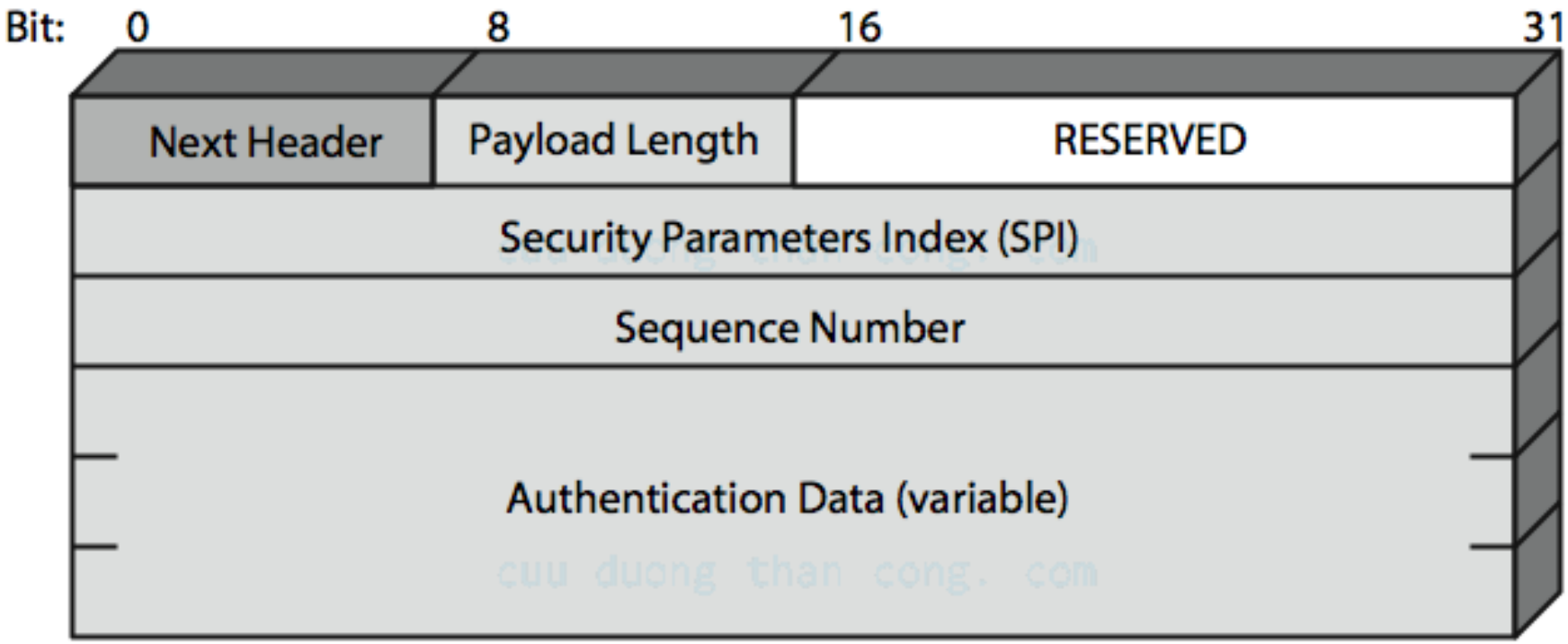
Các liên kết an ninh

- Khái niệm liên kết an ninh (SA)
  - Là quan hệ một chiều giữa bên gửi và bên nhận, cho biết các dịch vụ an ninh đối với luồng tin lưu chuyển
- Mỗi SA được xác định duy nhất bởi 3 tham số
  - Chỉ mục các tham số an ninh (SPI)
  - Địa chỉ IP đích
  - Định danh giao thức an ninh
- Các tham số khác lưu trong CSDL SA (SAD)
  - Số thứ tự, các thông tin AH và ESP, thời hạn,...
- CSDL chính sách an ninh (SPD) cho phép điều chỉnh mức độ áp dụng IPSec

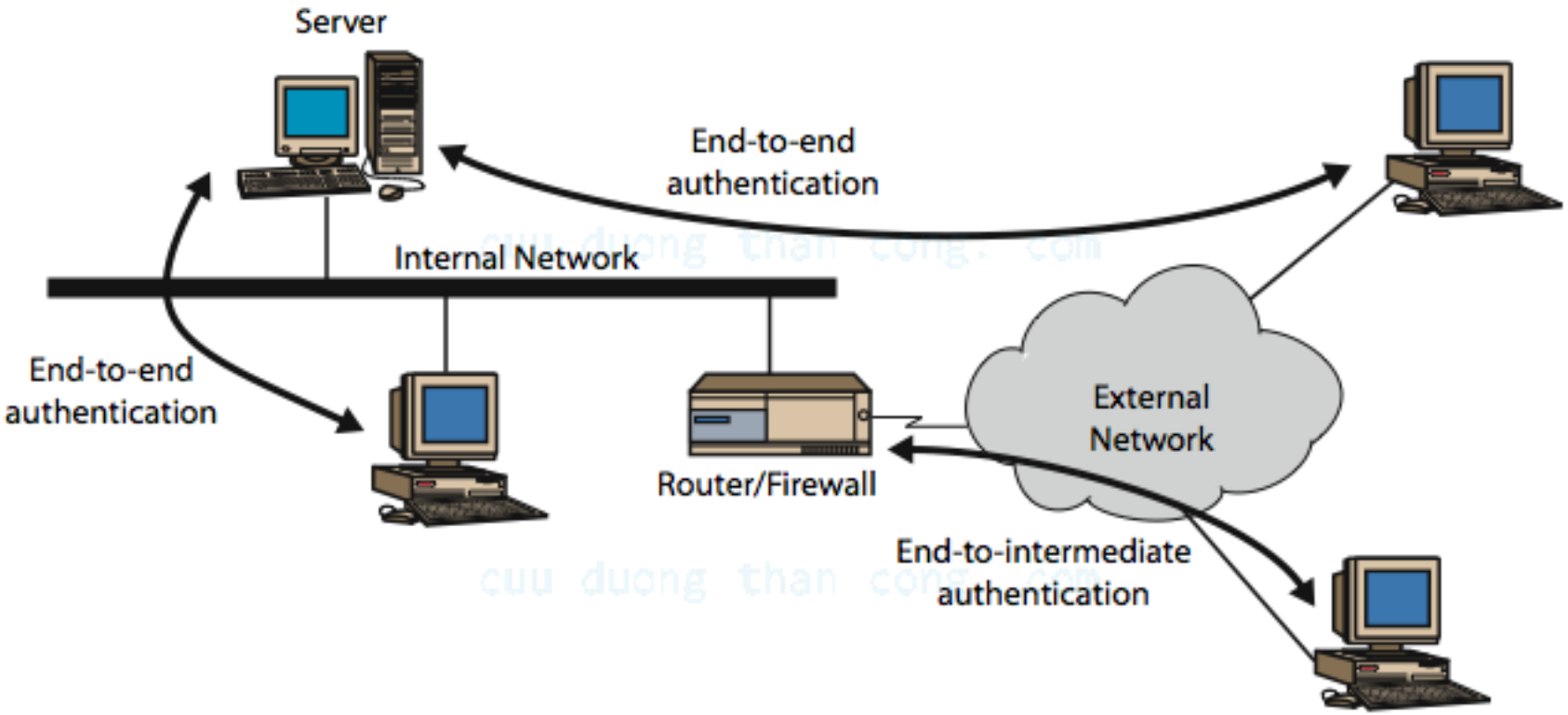
Phần đầu xác thực

- Đảm bảo toàn vẹn và xác thực các gói IP
  - Cho phép một hệ thống đầu cuối hay một thiết bị mạng xác thực người dùng hoặc ứng dụng
  - Tránh giả mạo địa chỉ nhờ xem xét số thứ tự
  - Chống lại hình thức tấn công lặp lại
- Sử dụng mã xác thực thông báo
- Bên gửi và bên nhận phải có một khóa bí mật dùng chung

Khuôn dạng AH



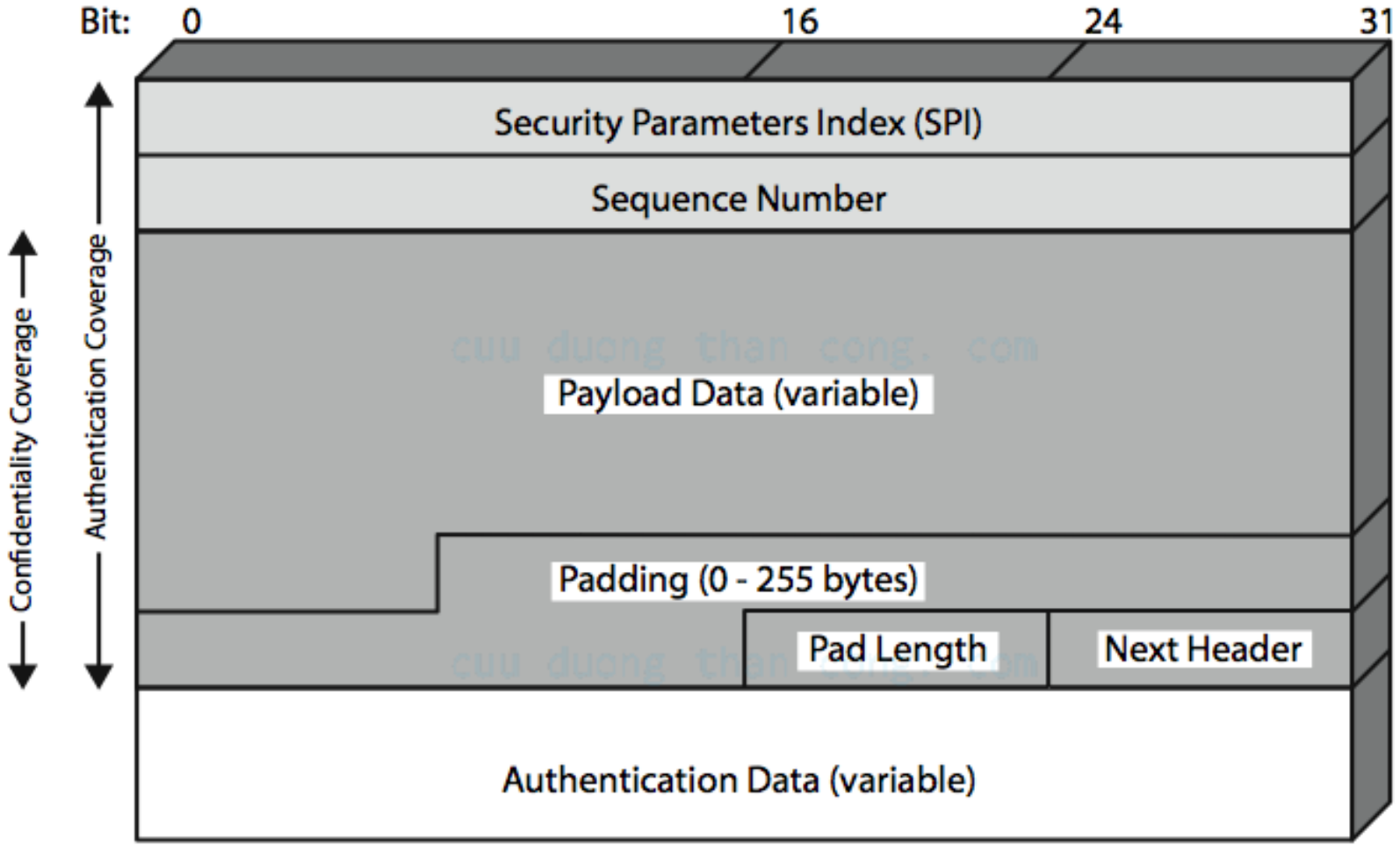
Chế độ giao vận và đường hầm



Phần đầu ESP

- Đảm bảo bảo mật nội dung và bảo mật luồng tin hữu hạn
- Có thể cung cấp các dịch vụ xác thực giống như với AH
- Cho phép sử dụng nhiều giải thuật mã hóa, phương thức mã hóa, và cách độn khác nhau
  - DES, 3DES, RC5, IDEA, CAST,...
  - CBC,...
  - Độn cho tròn kích thước khối, kích thước trường, che dấu lưu lượng luồng tin

Khuôn dạng ESP



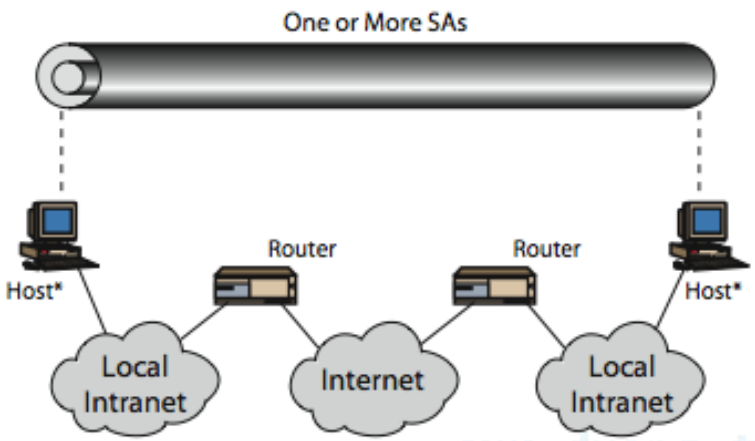
Giao vận và đường hầm ESP

- Chế độ giao vận ESP dùng để mã hóa và có thể có thêm chức năng xác thực dữ liệu IP
  - Chỉ mã hóa dữ liệu không mã hóa phần đầu
  - Dễ bị phân tích lưu lượng nhưng hiệu quả
  - Áp dụng cho truyền tải giữa hai điểm cuối
- Chế độ đường hầm mã hóa toàn bộ gói tin IP
  - Phải bổ xung phần đầu mới cho mỗi bước chuyển
  - Áp dụng cho các mạng riêng ảo, truyền tải thông qua cầu nối

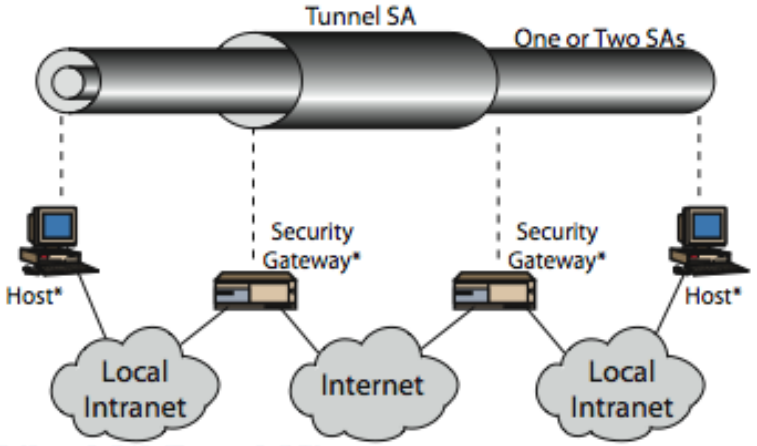
Kết hợp các liên kết an ninh

- Mỗi SA chỉ có thể cài đặt một trong hai giao thức AH và ESP
- Để cài đặt cả hai cần kết hợp các SA với nhau
  - Tạo thành một gói liên kết an ninh
  - Có thể kết thúc tại các điểm cuối khác nhau hoặc giống nhau
- Kết hợp theo 2 cách
  - Gần với giao vận
  - Tạo đường hầm theo nhiều bước
- Cần xem xét thứ tự xác thực và mã hóa

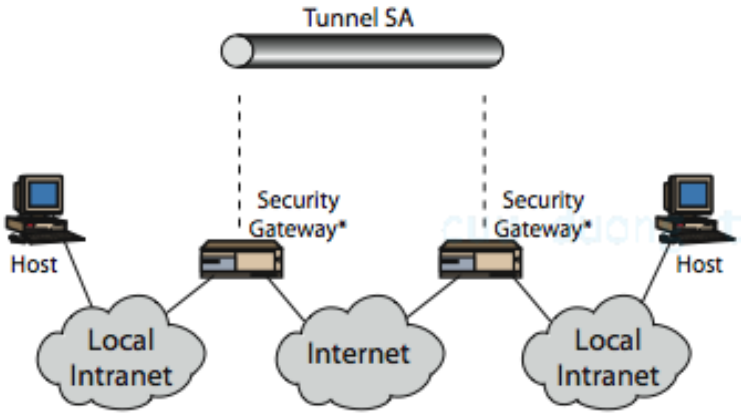
Ví dụ kết hợp các SA



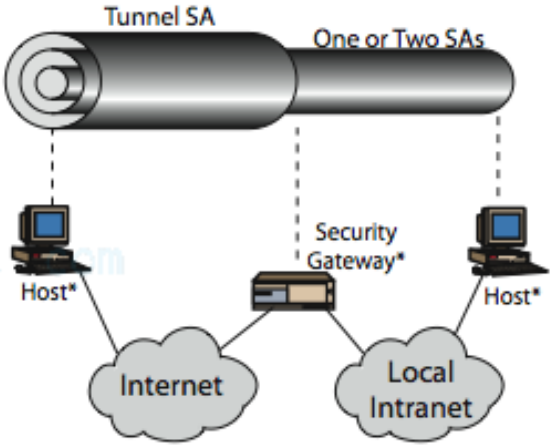
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

Quản lý khóa

- Có chức năng sản sinh và phân phối khóa
- Hai bên giao tiếp với nhau nói chung cần 4 khóa
  - Mỗi chiều cần 2 khóa: 1 cho AH, 1 cho ESP
- Hai chế độ quản lý khóa
  - Thủ công
    - Quản trị hệ thống khai báo các khóa khi thiết lập cấu hình
    - Thích hợp với các môi trường nhỏ và tương đối tĩnh
  - Tự động
    - Cho phép tạo khóa theo yêu cầu cho các SA
    - Thích hợp với các hệ phân tán lớn có cấu hình luôn thay đổi
    - Gồm các thành phần Oakley và ISAKMP

Oakley

- Là một giao thức trao đổi khóa dựa trên giải thuật Diffie-Hellman
- Bao gồm một số cải tiến quan trọng
  - Sử dụng cookie để ngăn tấn công gây quá tải
    - Cookie cần phụ thuộc vào các bên giao tiếp, không thể sinh ra bởi một bên khác với bên sinh cookie, có thể sinh và kiểm tra một cách nhanh chóng
  - Hỗ trợ việc sử dụng các nhóm với các tham số Diffie-Hellman khác nhau
  - Sử dụng các giá trị nonce để chống tấn công lặp lại
  - Xác thực các trao đổi Diffie-Hellman để chống tấn công người ở giữa

ISAKMP

- Viết tắt của Internet Security Association and Key Management Protocol
- Cung cấp một cơ cấu cho việc quản lý khóa
- Định nghĩa các thủ tục và các khuôn dạng thông báo cho việc thiết lập, thỏa thuận, sửa đổi, và hủy bỏ các liên kết an ninh
- Độc lập với giao thức trao đổi khóa, giải thuật mã hõa, và phương pháp xác thực

Các khuôn dạng ISAKMP