Chương 5.
Công nghệ mạng riêng ảo

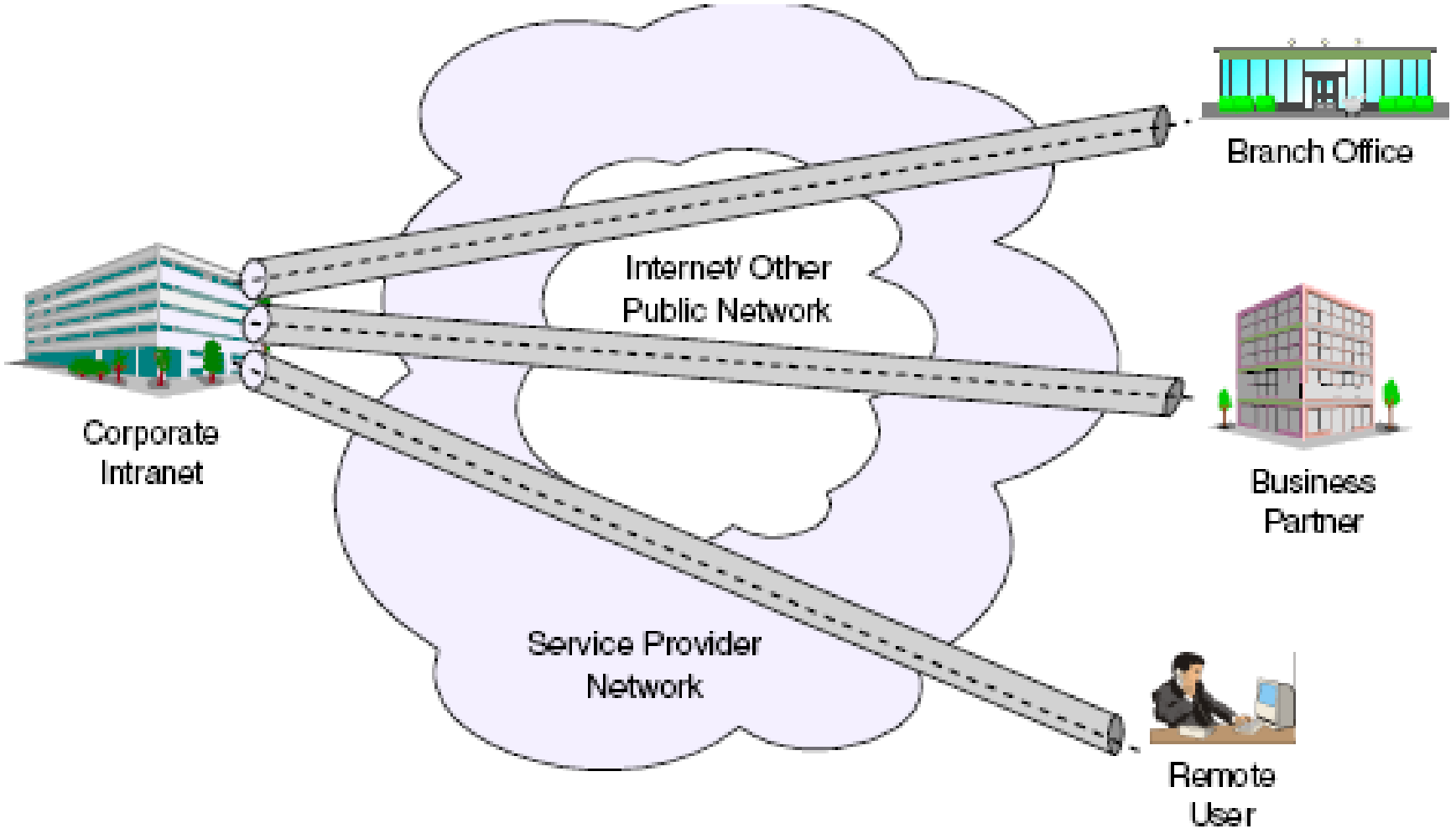
I. Giới thiệu chung

- Mạng riêng ảo – Virtual Private Network
- VPN là phương pháp đảm bảo an toàn truy cập từ xa bằng phương pháp thiết lập kênh kết nối riêng (private) trên môi trường mạng công cộng (Internet).

I. Giới thiệu chung

- “Mạng riêng ảo”:
  - “Mạng riêng”: Chỉ có công ty thiết lập nên nó mới sử dụng được.
  - “Ảo”: Kênh truyền riêng trên mạng Internet

Kết nối VPN


Branch Office
Internet/ Other
Public Network
Corporate
Intranet
Business
Partner
Service Provider
Network
Remote
User

I. Giới thiệu chung

- Thành phần mạng VPN:
  - LAN chính tại trụ sở chính
  - LAN phụ tại chi nhánh
  - Người dùng từ xa, Home network
  - Khách hàng, đối tác
  - Đường truyền Internet
  - Máy chủ VPN

I. Giới thiệu chung

- Ưu điểm:
  - Chi phí thấp
  - Tăng cường tính bảo mật cho hệ thống
  - Tính mở rộng và linh động
  - Giảm chi phí vận hành và quản lý

I. Yêu cầu an toàn

- Bảo mật:
  - Thực thi giải pháp phòng thủ
  - Xác thực
  - Mã hóa dữ liệu
  - Quản lý khóa

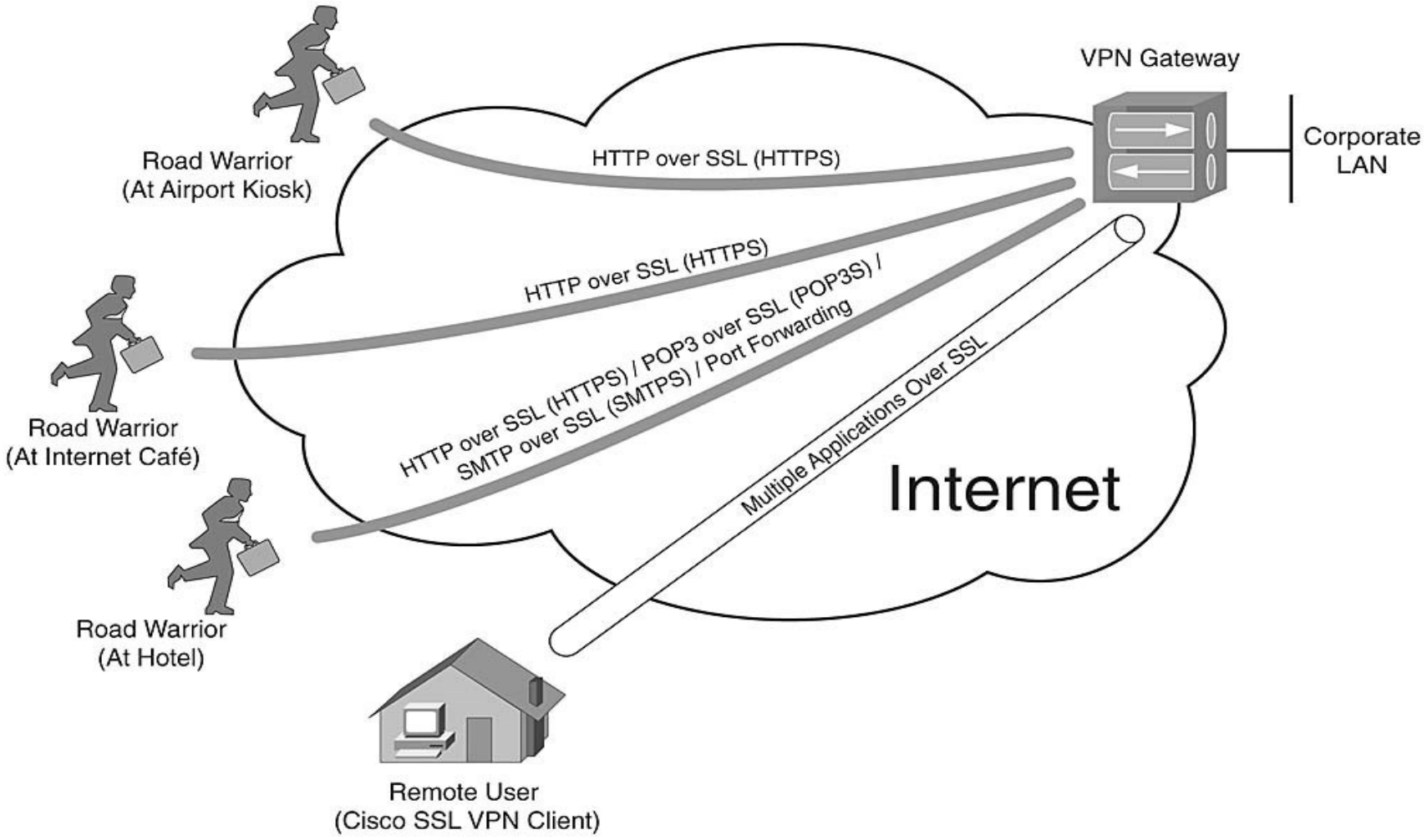
I. Yêu cầu an toàn

- Sẵn sàng và tin cậy:
  - Khả năng định tuyến
  - Dư thừa các đường truy cập
  - Thiết bị dự phòng khi có lỗi phát sinh

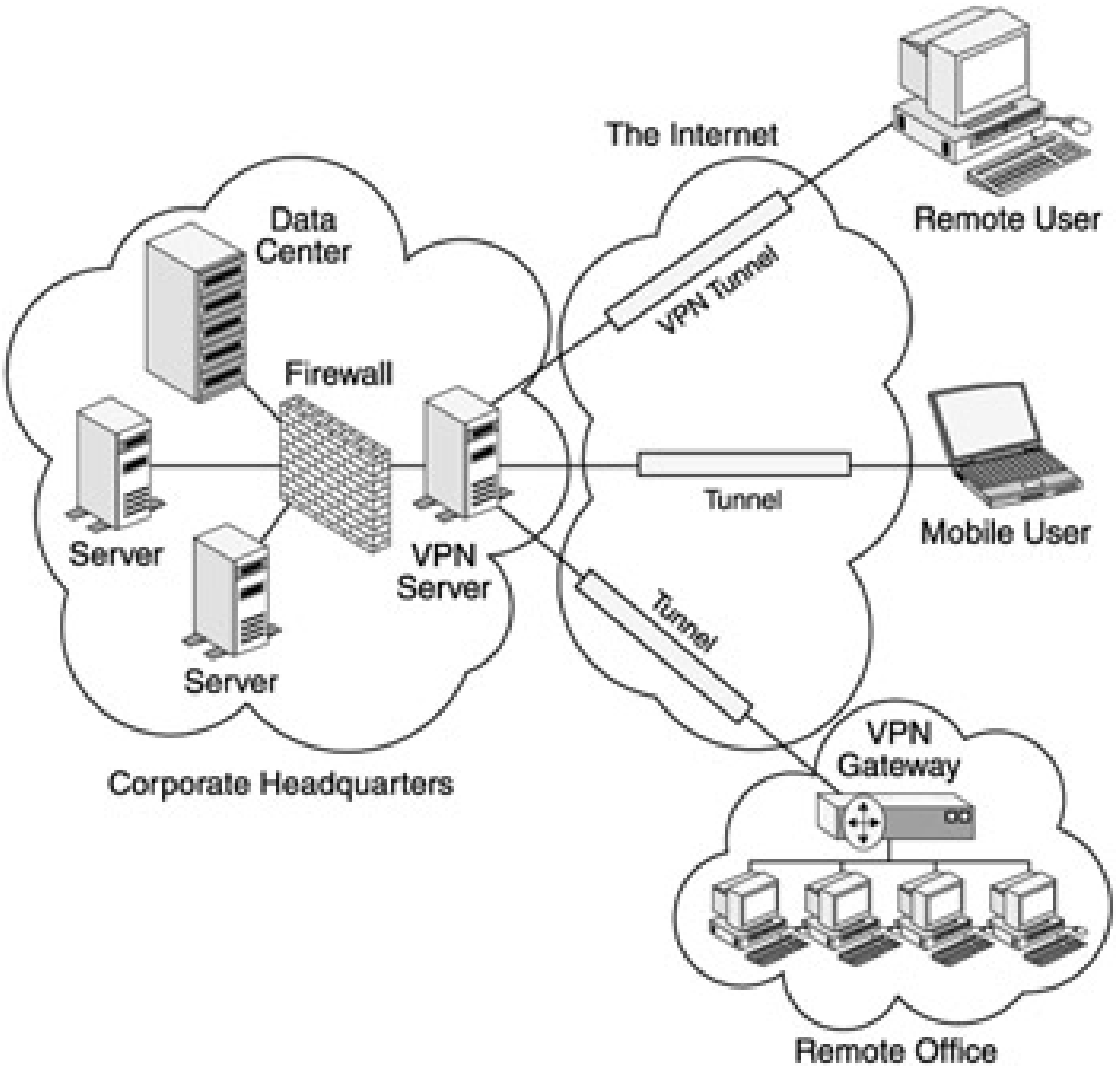
2. Phân loại mạng VPN

- Mạng VPN có 2 loại hình:
  - VPN Client-to-Site
  - VPN Site-to-Site

VPN Client-to-Site



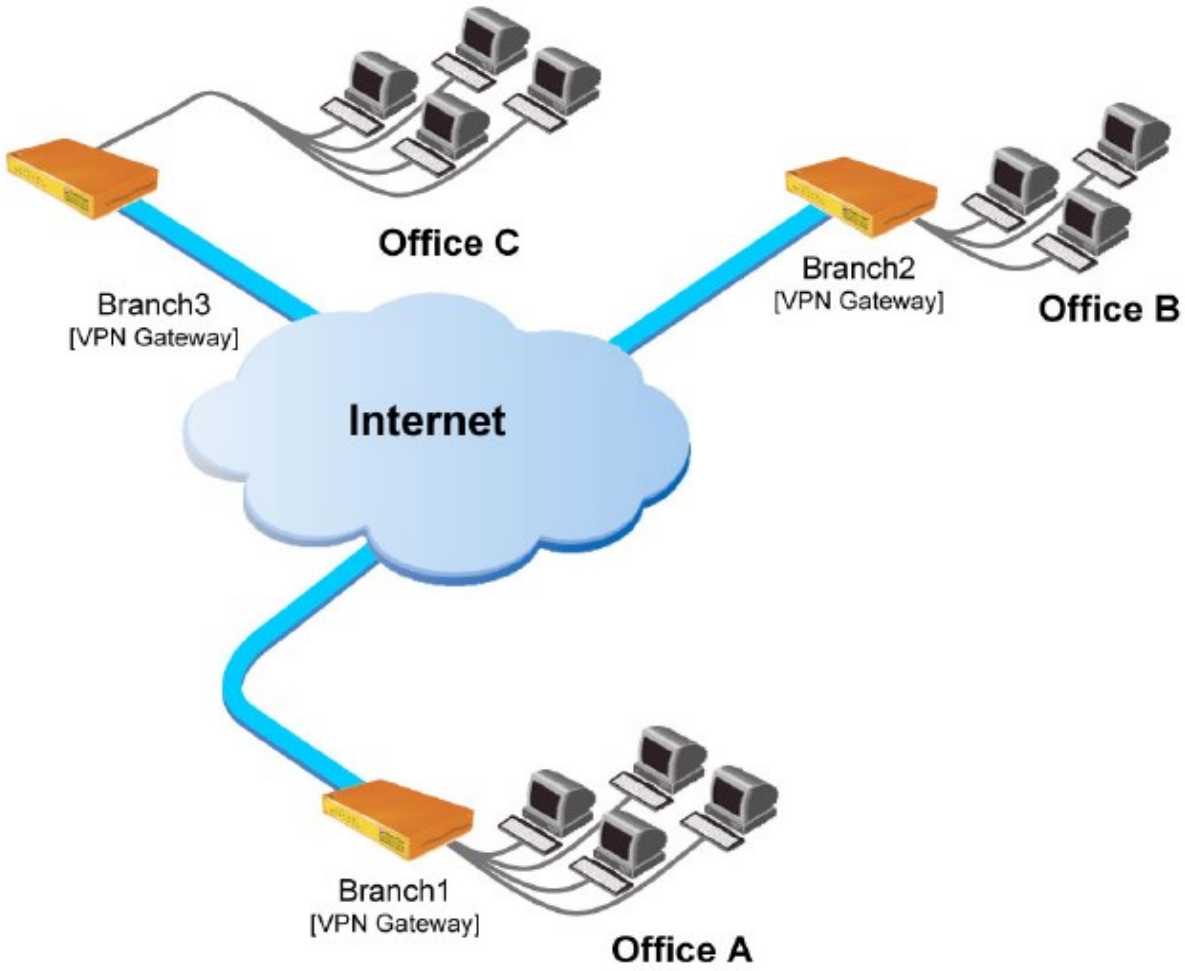
VPN Client-to-Site



VPN Client-to-Site

- VPN Remote Access
- Cung cấp dịch vụ truy cập từ xa cho người dùng
- Cho phép người dùng truy cập tới tài nguyên nội bộ khi đã kết nối
- Yêu cầu: Người dùng cần có tài khoản truy cập VPN để xác thực.
- Đường kết nối Internet vào máy chủ dịch vụ VPN

VPN Site-to-Site



VPN Site-to-Site

- Kết nối mạng ở các nơi khác nhau tạo thành một hệ thống mạng thống nhất.

Các giao thức bảo mật trong VPN

- Giao thức điểm nối điểm: PPTP
- Giao thức bảo mật lớp 2: L2TP
- Giao thức bảo mật tầng IP: IPSec
- Giao thức bảo mật tầng ứng dụng: SSL/TLS
- Giao thức xác thực: RADIUS

Giao thức PPTP

- Giao thức tạo đường hầm điểm nối điểm (PPTP - Point to Point Tunneling Protocol):
  - Giao thức cơ bản dựa vào PPP.
  - PPP payload được mã hóa sử dụng giao thức MPPE. Sử dụng RSA, RC4 với khóa phiên có độ dài lớn nhất 128 bít.
  - Lỗ hổng trong giao thức xác thực MSCHAP-v2
  - Tuy nhiên giao thức này có tốc độ mã hóa nhanh.
  - Hệ điều hành hỗ trợ: Windows, Mac OSX, Linux, iOS, Android.

Giao thức PPTP

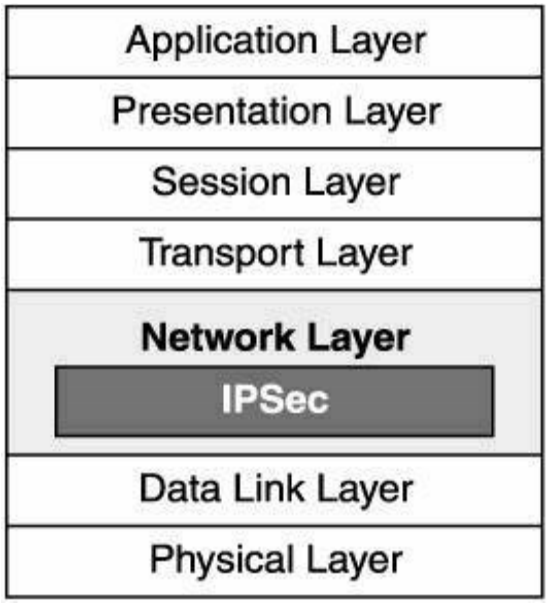
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fe80::f9bb:1841:36f	ff02::1:2	DHCPv6	150	Solicit XID: 0xc44295 CI
2	8.45306000	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
3	8.45387300	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
4	8.54803300	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP
5	9.46926300	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
6	9.47014700	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
7	9.57792800	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP
8	10.4834860	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
9	10.4844640	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
10	10.5921200	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP
11	11.4817260	192.168.1.20	192.168.1.1	PPP Con	111	Compressed data
12	11.4827690	192.168.1.1	192.168.1.20	PPP Con	115	Compressed data
13	11.5902690	192.168.1.20	192.168.1.1	GRE	60	Encapsulated PPP

Giao thức L2TP

- Giao thức đường hầm lớp 2 (L2TP – Layer 2 Tunneling Protocol):
  - Giao thức mã hóa nâng cao
  - L2TP payload được má hóa thông qua 3DES, AES
  - Thường kết hợp với giao thức IPSec
  - Hệ điều hành hỗ trợ: Windows, Mac OSX, Linux, iOS, Android

Giao thức IPSec

- Giới thiệu:
  - **IPSec** (Internet Protocol Security): Nó có quan hệ tới một số bộ giao thức (AH, ESP, và một số chuẩn khác) được phát triển bởi Internet Engineering Task Force (IETF).
  - Mục đích chính của việc phát triển IPSec là cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI.

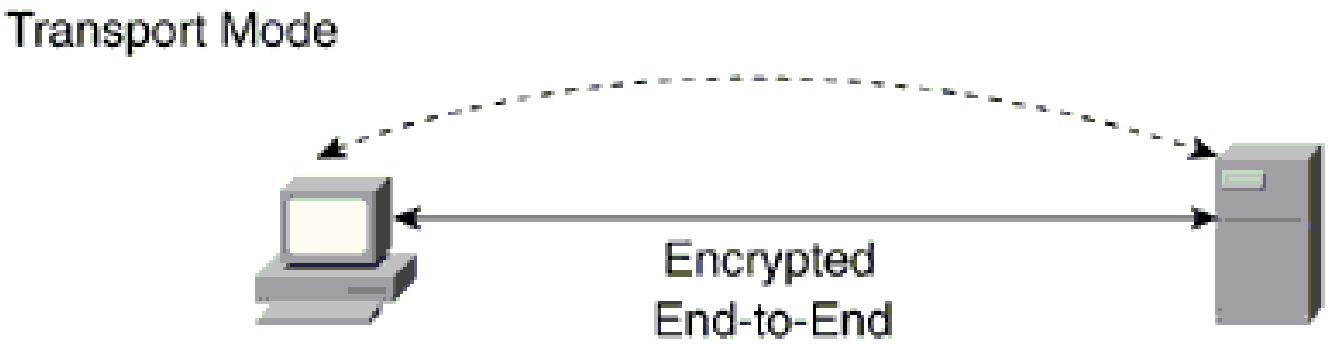


Giao thức IPSec

- Các giao thức con:
  - **AH** (*Authentication Header*): Được sử dụng để xác định nguồn gốc gói tin IP và đảm bảo tính toàn vẹn của nó.
  - **ESP** (*Encapsulating Security Payload*): được sử dụng để chứng thực và mã hóa gói tin IP (phần payload hoặc cả gói tin)
  - IKE (Internet Key Exchange): được sử dụng để thiết lập khóa bí mật cho người gửi và người nhận.

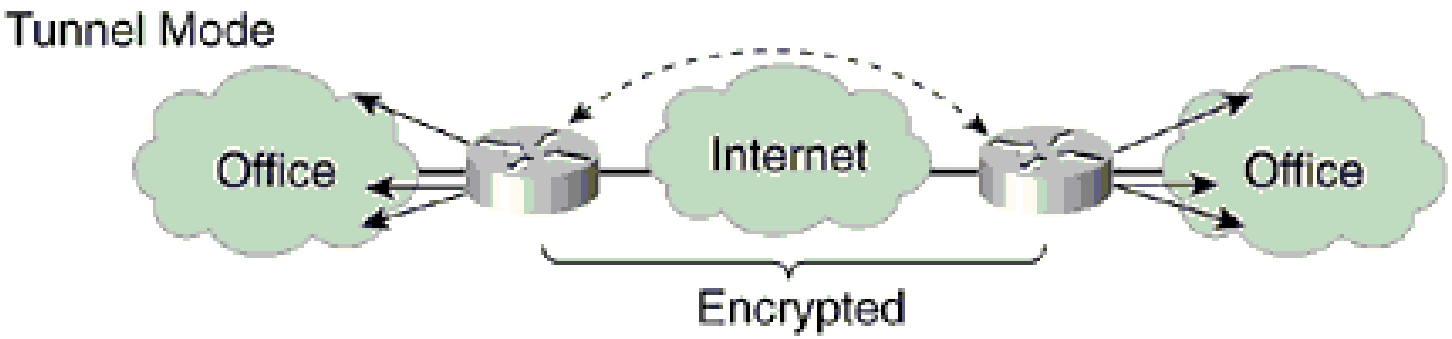
Giao thức IPSec

- Các chế độ hoạt động của IPsec:
  - **Chế độ vận chuyển** (transport mode): Bảo vệ đường truyền kết nối chỉ riêng giữa các Host.



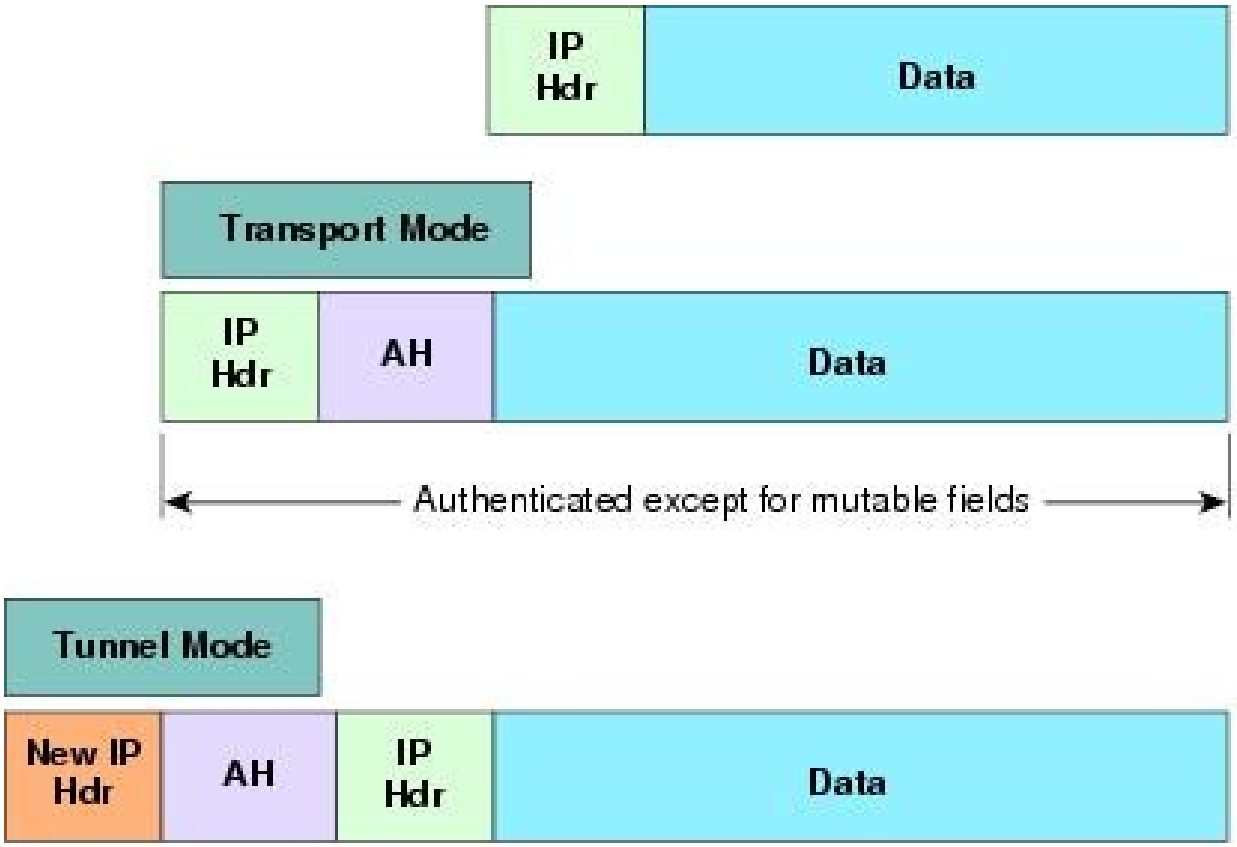
Giao thức IPSec

- **Chế độ đường hầm** (tunnel mode): Bảo vệ đường truyền kết nối giữa các mạng nội bộ với nhau.



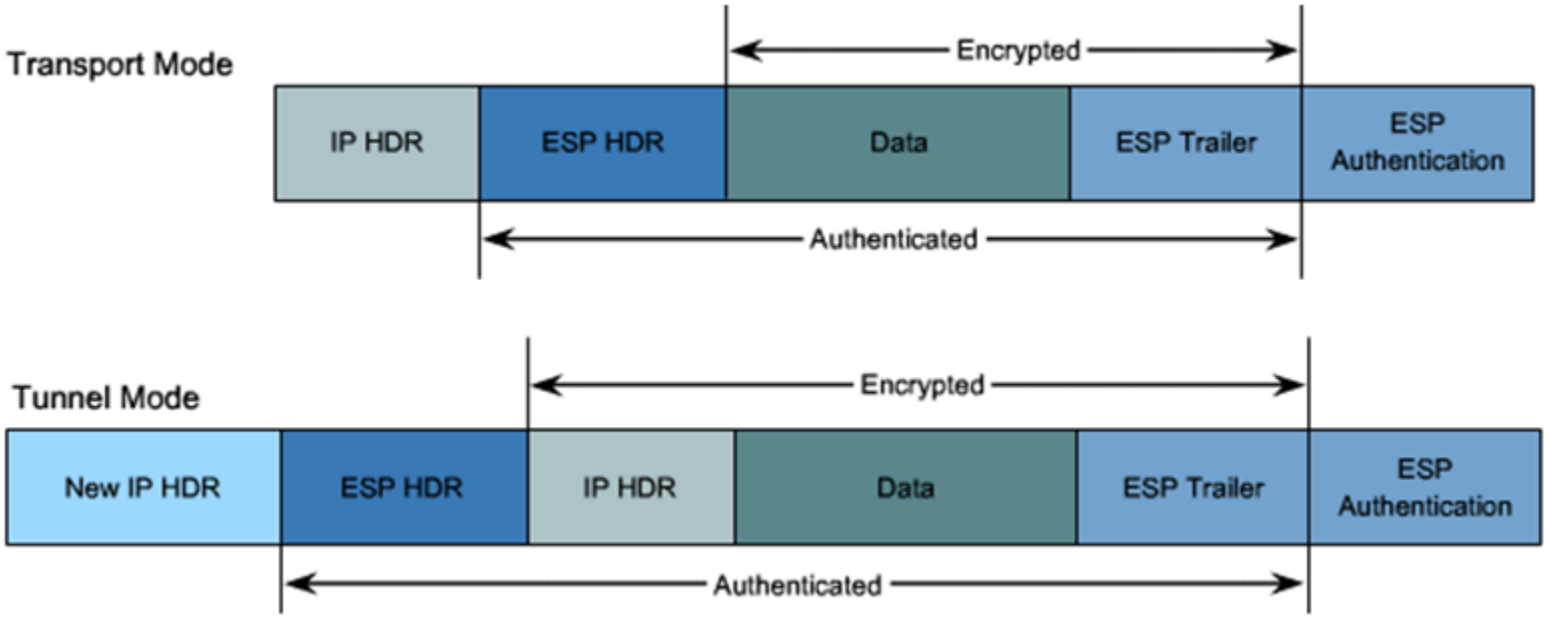
Giao thức IPSec

- Gói tin của AH:



Giao thức IPSec

- Định dạng gói tin của ESP:



Giao thức IPSec

- Các hệ mật sử dụng trong IPSec:
  - Thuật toán mã hóa: DES, 3DES.
  - Toàn vẹn dữ liệu: MD5, SHA-1
  - Xác thực: Kerberos, chứng thư số, khóa chia sẻ.

Giao thức IPSec

No.	Time	Source	Destination	Protocol
1	0.00000000	Vmware_b8:c3:80	Vmware_27:72:af	ARP
2	0.00051400	Vmware_27:72:af	Vmware_b8:c3:80	ARP
3	0.28401500	192.168.1.20	192.168.1.1	ESP
4	0.28499800	192.168.1.1	192.168.1.20	ESP
5	1.29857400	192.168.1.20	192.168.1.1	ESP
6	1.29969800	192.168.1.1	192.168.1.20	ESP
7	2.29656500	192.168.1.20	192.168.1.1	ESP
8	2.29750300	192.168.1.1	192.168.1.20	ESP
9	3.31023600	192.168.1.20	192.168.1.1	ESP
10	3.31109600	192.168.1.1	192.168.1.20	ESP
11	4.32440300	192.168.1.20	192.168.1.1	ESP
12	4.32534400	192.168.1.1	192.168.1.20	ESP
13	5.33850300	192.168.1.20	192.168.1.1	ESP

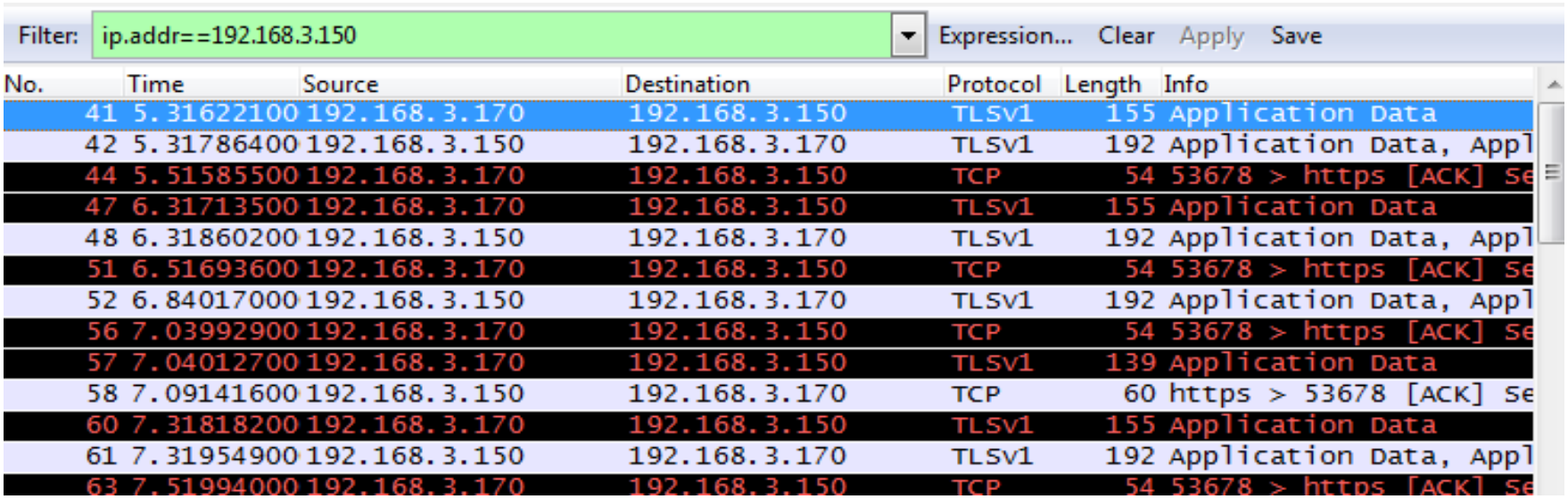
Giao thức VPN SSTP

- **Secure Socket Tunneling Protocol** (**SSTP**) is a form of virtual private network (VPN) tunnel that provides a mechanism to transport PPP traffic through an SSL/TLS channel.
- SSL/TLS provides transport-level security with key negotiation, encryption and traffic integrity checking.
- The use of SSL/TLS over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers except for authenticated web proxies.

Giao thức VPN SSTP

- SSTP servers must be authenticated during the SSL/TLS phase.
- SSTP clients can optionally be authenticated during the SSL/TLS phase and must be authenticated in the PPP phase.
- The use of PPP allows support for common authentication methods, such as EAP-TLS and MS-CHAP.
- SSTP is available for Linux, BSD, and Windows.

Giao thức VPN SSTP



Giao thức RADIUS