CHƯƠNG IX

MẠNG RIÊNG ẢO

(VPN - VIRTUAL PRIVATE NETWORK)

ThS. Nguyễn Cao Đạt

E-mail: dat@hcmut.edu.vn

Tham khảo

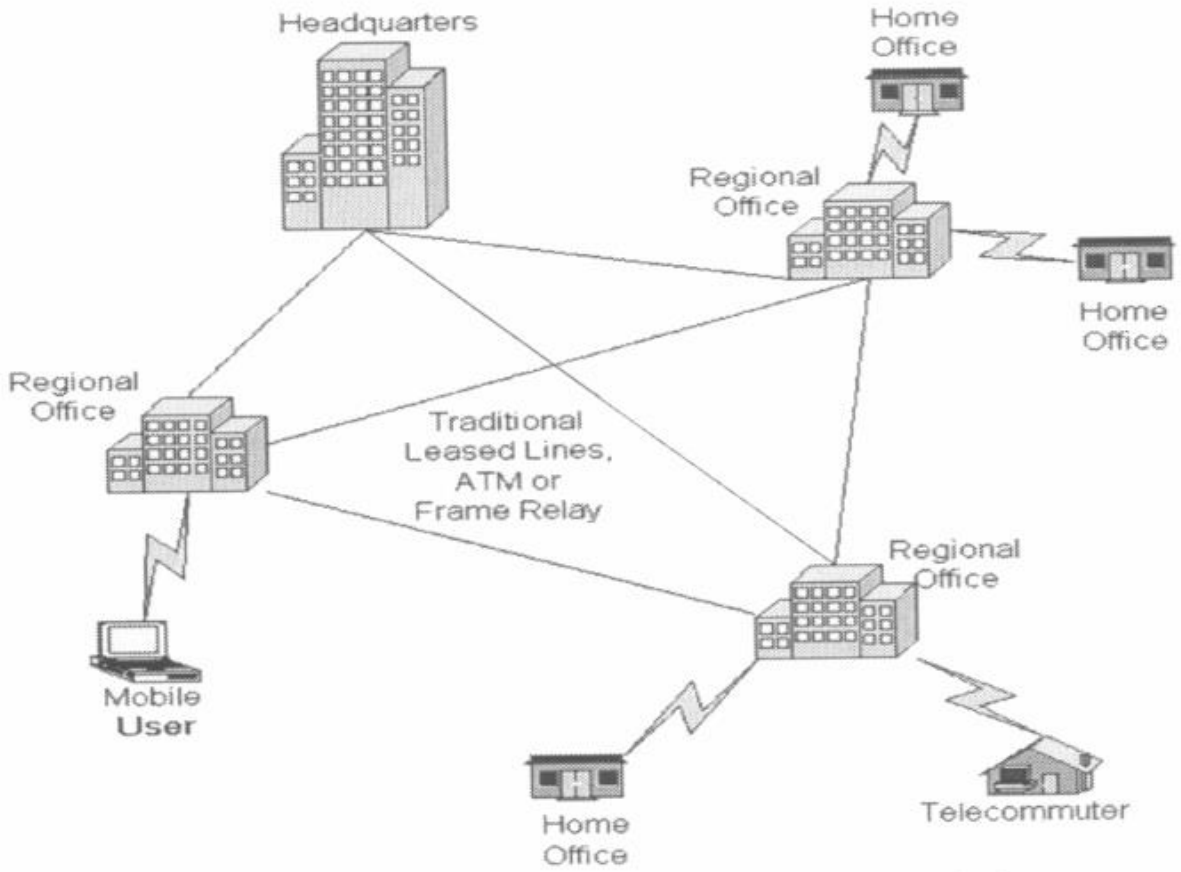
[2]. Network Security – A Beginner's Guide: module 11

Nội dung trình bày

- Khái niệm về mạng riêng ảo
- Cơ chế hoạt động
- Phân loại các hệ thống VPN
- Các thành phần chính của VPN
- Các loại trang thiết bị hỗ trợ VPN

Khái niệm về mạng riêng ảo

- **Vấn đề kết nối mạng truyền thống**



Khái niệm về mạng riêng ảo

- **VPN(Virtual Private Network) là một loại mạng riêng sử dụng môi trường truyền thông công cộng như Internet, thay vì dùng đường thuê bao (leased line) để truyền thông.**
- VPN trở nên phổ biến vì ngày càng nhiều người làm việc ở nhà, các vị trí xa trụ sở chính của công ty.

Khái niệm về mạng riêng ảo

Khái niệm về mạng riêng ảo

- **Ưu điểm của mạng riêng ảo**
  - Người dùng có thể truy cập mạng cục bộ từ các vị trí ở xa.
  - Internet được dùng như là trục xương sống cho mạng riêng ảo.
  - Giảm chi phí nhờ sử dụng thiết bị rẻ tiền hơn và giảm chi phí thuê bao/bảo trì đường truyền.
  - Có khả năng mở rộng.

Khái niệm về mạng riêng ảo

- **Các đặc điểm**
  - Thông tin được mã hóa để ngăn chặn việc nghe trộm.
  - Các site từ xa phải xác thực khi tạo kết nối.
  - Nhiều giao thức được hỗ trợ trên VPN.
  - Kết nối VPN là kết nối điểm điểm.

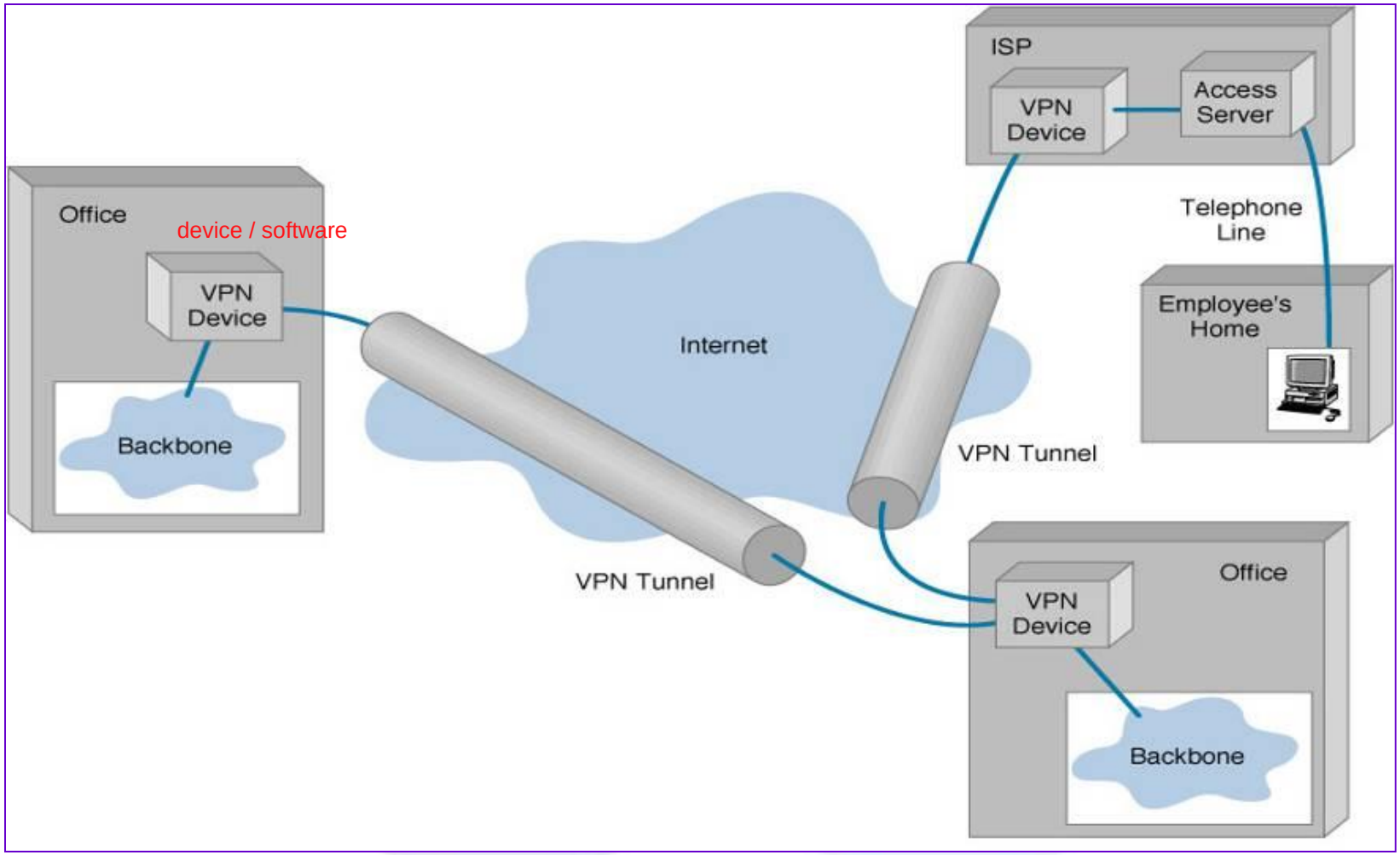
Khái niệm về mạng riêng ảo

- **Các chức năng**
  - Xác thực: Kiểm tra tính hợp lệ của dữ liệu được gởi từ một nguồn nào đó.
  - Quản lý truy cập: Giới hạn các người dùng không có quyền truy cập đến mạng cục bộ.
  - Bí mật, riêng tư: Tránh việc đọc hay sao chép dữ liệu trong quá trình vận chuyển.
  - Toàn vẹn: Chắc chắn dữ liệu không bị thay đổi trong quá trình vận chuyển.

Cơ chế hoạt động

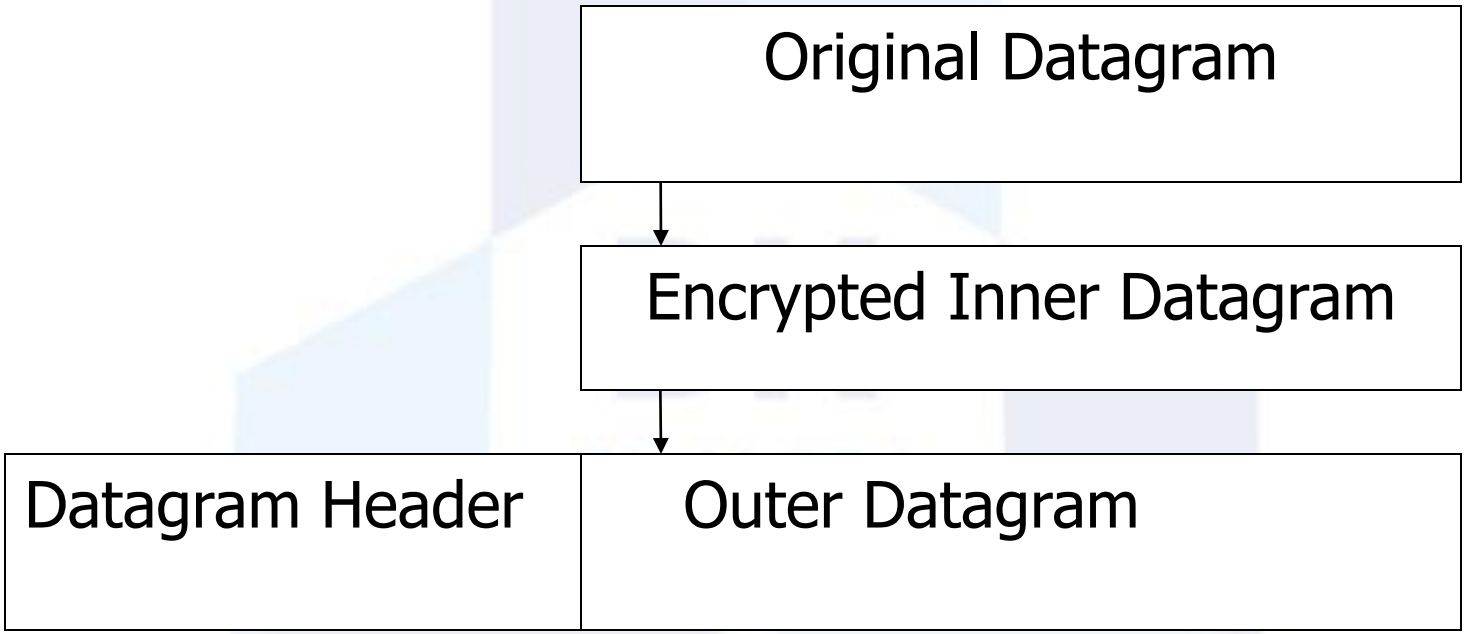
- **Gồm có hai kết nối**
  - Một kết nối đến Internet
  - Một kết nối ảo VPN
- **Sử dụng các giao thức**
  - Để tạo các đường hầm VPN (VPN tunnels).

Cơ chế hoạt động



Kỹ thuật đường hầm VPN

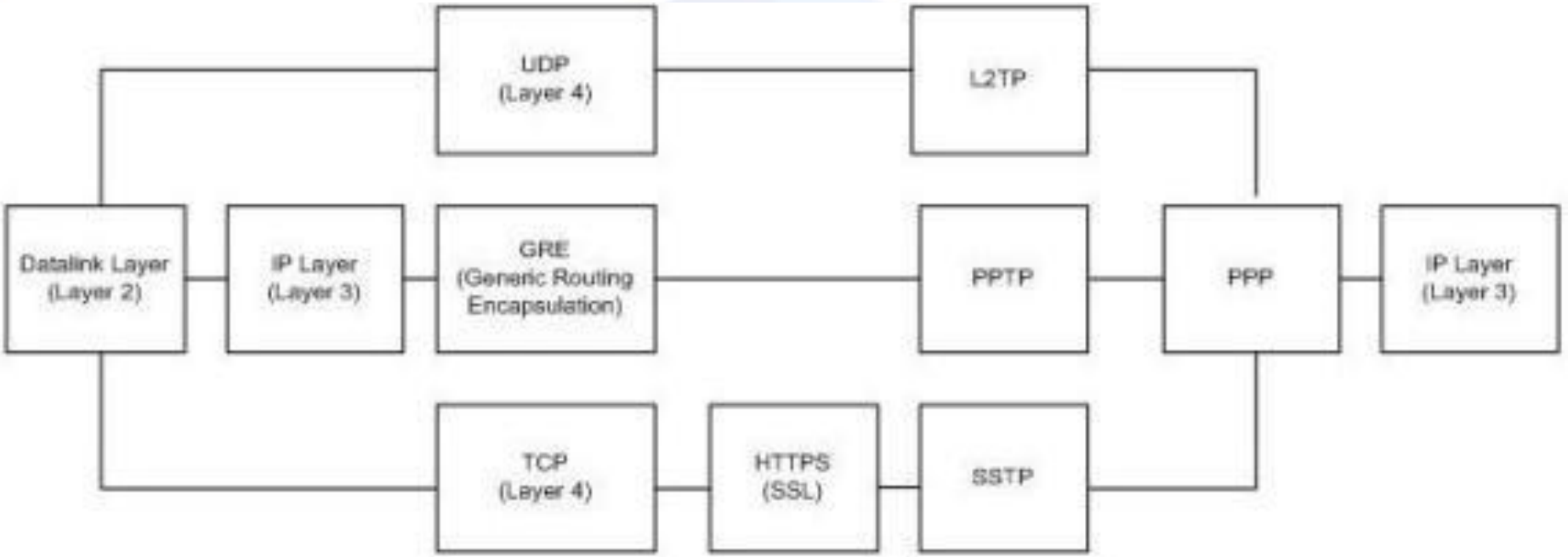
- Một kết nối ảo điểm – điểm được tạo thông qua mạng công cộng. Nó vận chuyển các gói tin đã được đóng gói.



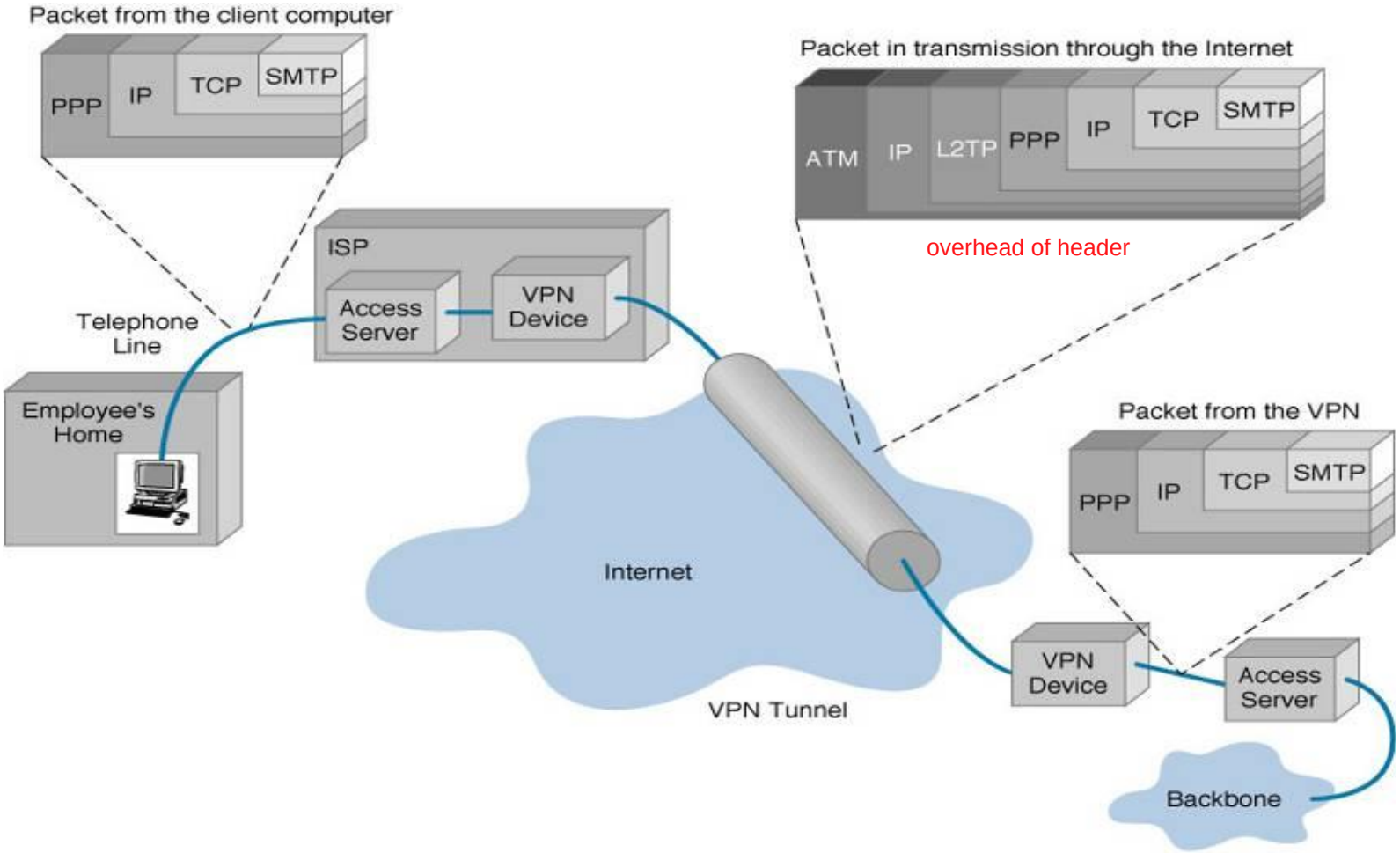
Các giao thức được dùng trong VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security
- VPN over SSL (SSTP)

Các giao thức được dùng trong VPN



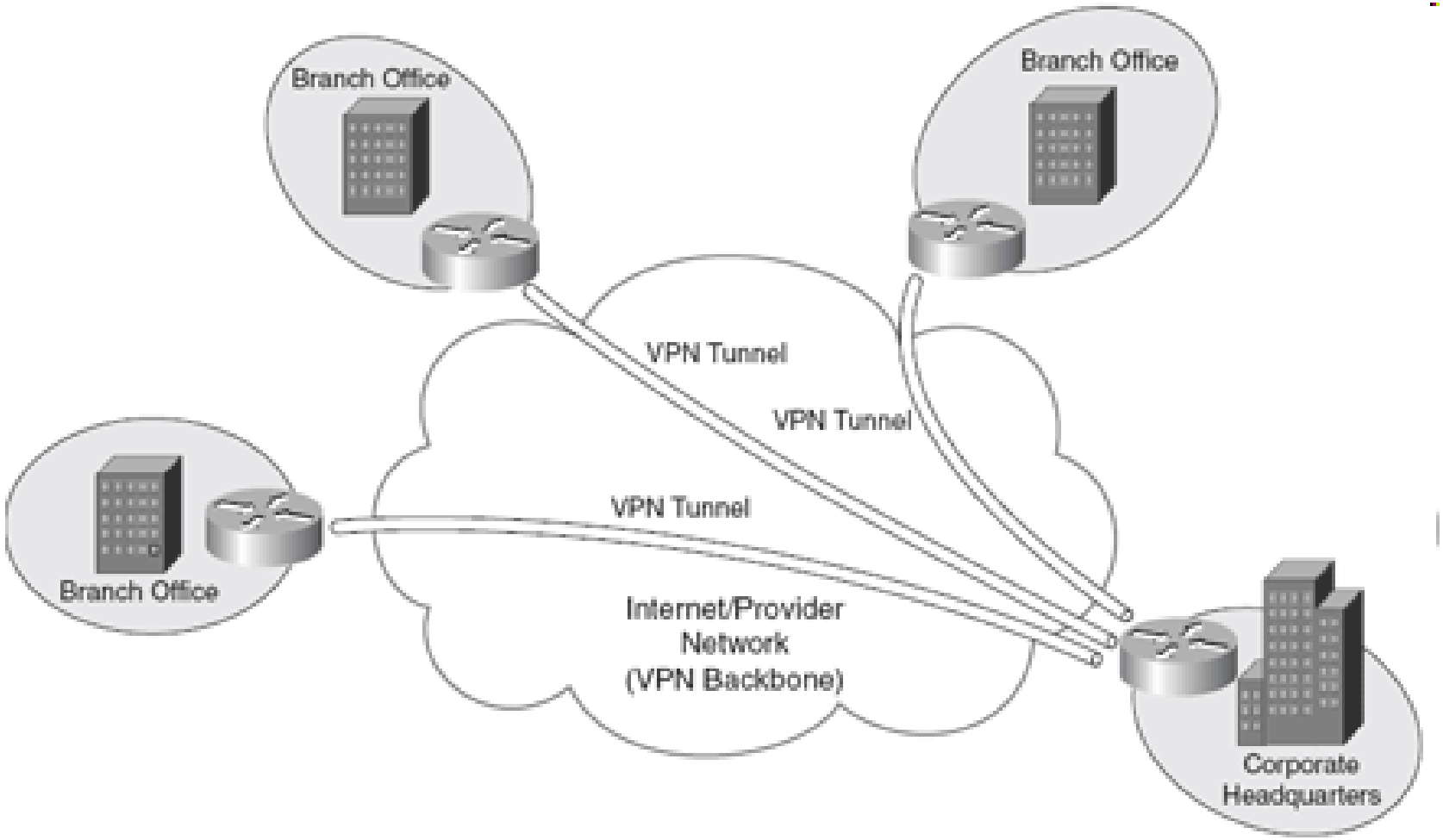
Việc đóng gói của các gói tin



Phân loại các hệ thống VPN

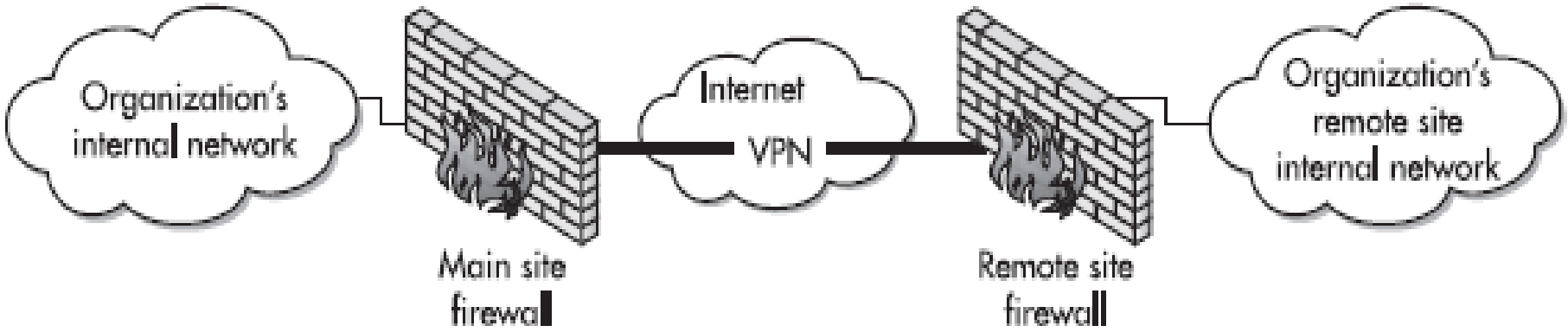
- **Phân biệt dựa trên cách thức sử dụng**
- **Bao gồm hai loại**
  - Site to Site VPN
  - User VPN

Site to Site VPN



Site to Site VPN

- Được dùng để kết nối các site ở xa mà không cần dùng đường thuê bao đắt tiền hay kết nối hai tổ chức khác nhau cho mục đích kinh doanh, hợp tác.
- Thông thường VPN được tạo bằng cách kết nối một firewall hay bộ định tuyến biên đến một firewall hay bộ định tuyến biên khác.



Lợi ích của Site to Site VPN

- Chi phí thuê bao cũng như bảo trì được giảm đáng kể
- Hạ tầng mạng cũng được triển khai nhanh hơn nếu các ISP cục bộ cung cấp các kết nối ISDN hay DSL cho các site ở xa.
- Các quy tắc cũng được thiết lập dựa trên chính sách của tổ chức cho việc làm thế nào để các site ở xa kết nối đến site trung tâm hay giữa chúng với nhau.
- Nếu kết nối giữa hai tổ chức thì các hạn chế nghiêm ngặt trong việc truy cập mạng nội bộ và các hệ thống máy tính cũng dễ dàng thiết lập.

Các vấn đề của Site to Site VPN

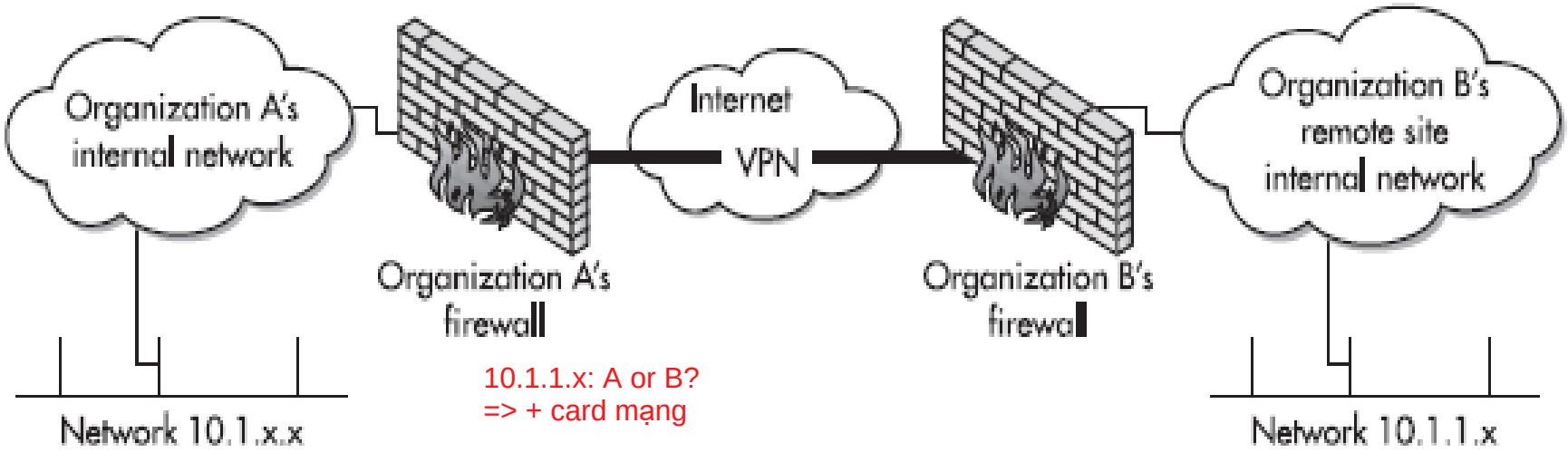
- Site to Site VPN dùng cho một tổ chức
  - Vành đai an ninh của tổ chức được mở rộng vì vậy phải đảm bảo các chính sách mạnh mẽ và các chức năng kiểm soát được thực thi trong toàn bộ các site.

- Site to Site VPN dùng giữa hai tổ chức
  - Các chính sách bảo mật trên mỗi đầu kết nối rất quan trọng.
  - Cả hai tổ chức cần phải xác định những gì được và không được phép qua VPN và thiết lập chính sách bức tường lửa của họ cho phù hợp.

Các vấn đề của Site to Site VPN

- Vấn đề chứng thực VPN
  - Khóa bí mật dùng chung vì vậy không nên dùng chung cho nhiều kết nối VPN
  - Nếu chứng chỉ khóa công khai được dùng thì các thủ tục phải được tạo ra để xử lý khi chứng chỉ thay đổi hay hết hạn
- Vấn đề quá tải trên VPN Server nếu lưu lượng truy cập cao do phải mã hóa/giải mã dữ liệu
- Vấn đề xung đột vùng địa chỉ sử dụng

Các vấn đề của Site to Site VPN

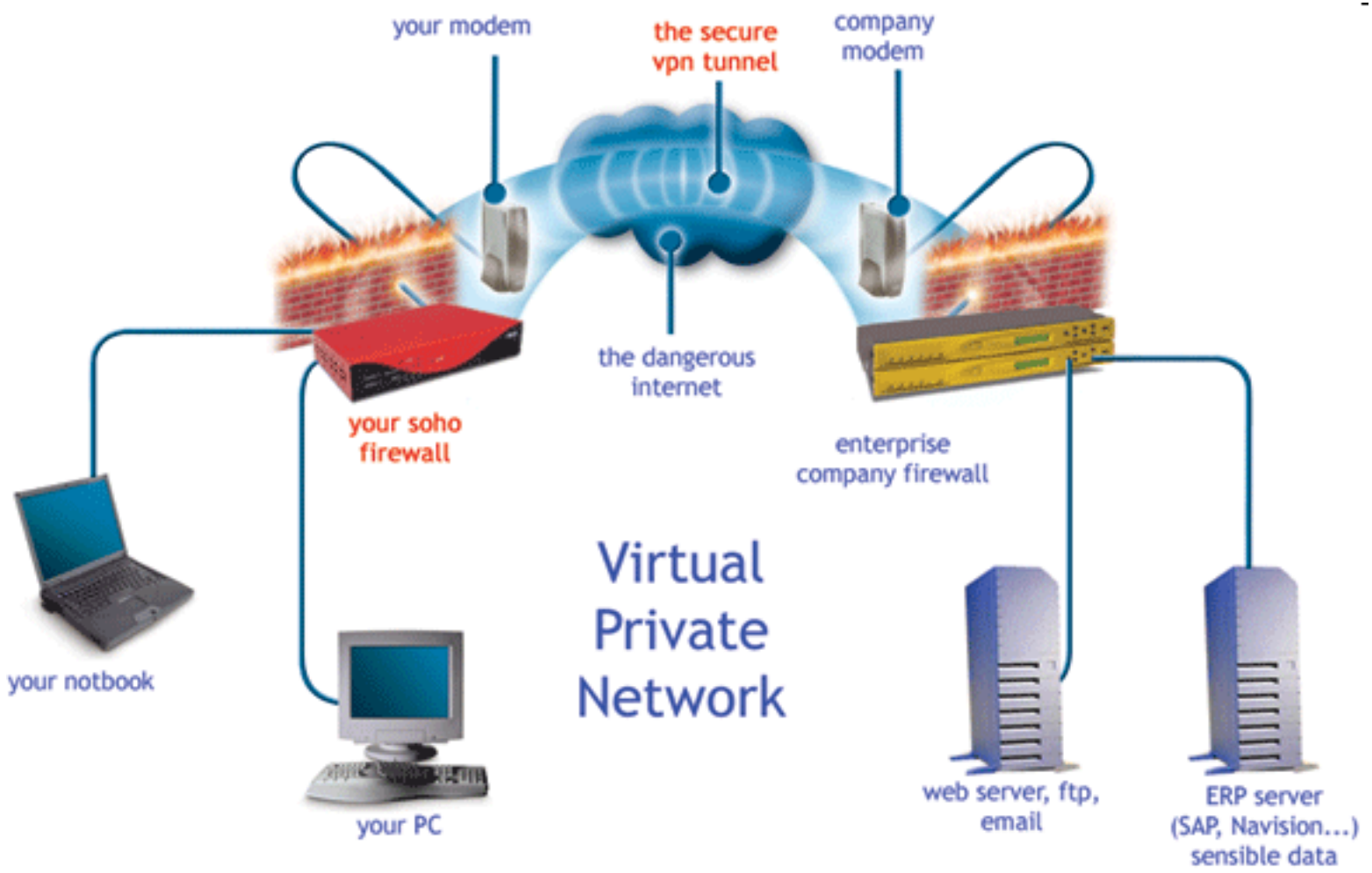


10.1.1.x: A or B?
=> + card mạng

Quản lý Site to Site VPN

- Sau khi thành lập, Site to Site VPN cần được giám sát để đảm bảo thông suốt.
- Các quy tắc liên quan với Site to Site VPN cũng cần được kiểm tra định kỳ để đảm bảo rằng nó phù hợp với chính sách tổ chức.
- Vấn đề định tuyến cũng cần được kiểm soát. Các tuyến đường đến site từ xa phải được tạo ra trên các bộ định tuyến mạng nội bộ nên các tuyến đường này không được xóa trong quá trình bảo trì định tuyến.

User VPN


your modem
the secure vpn tunnel
company modem
the dangerous internet
your soho firewall
enterprise company firewall
Virtual Private Network
your notbook
your PC
web server, ftp, email
ERP server (SAP, Navision...) sensible data

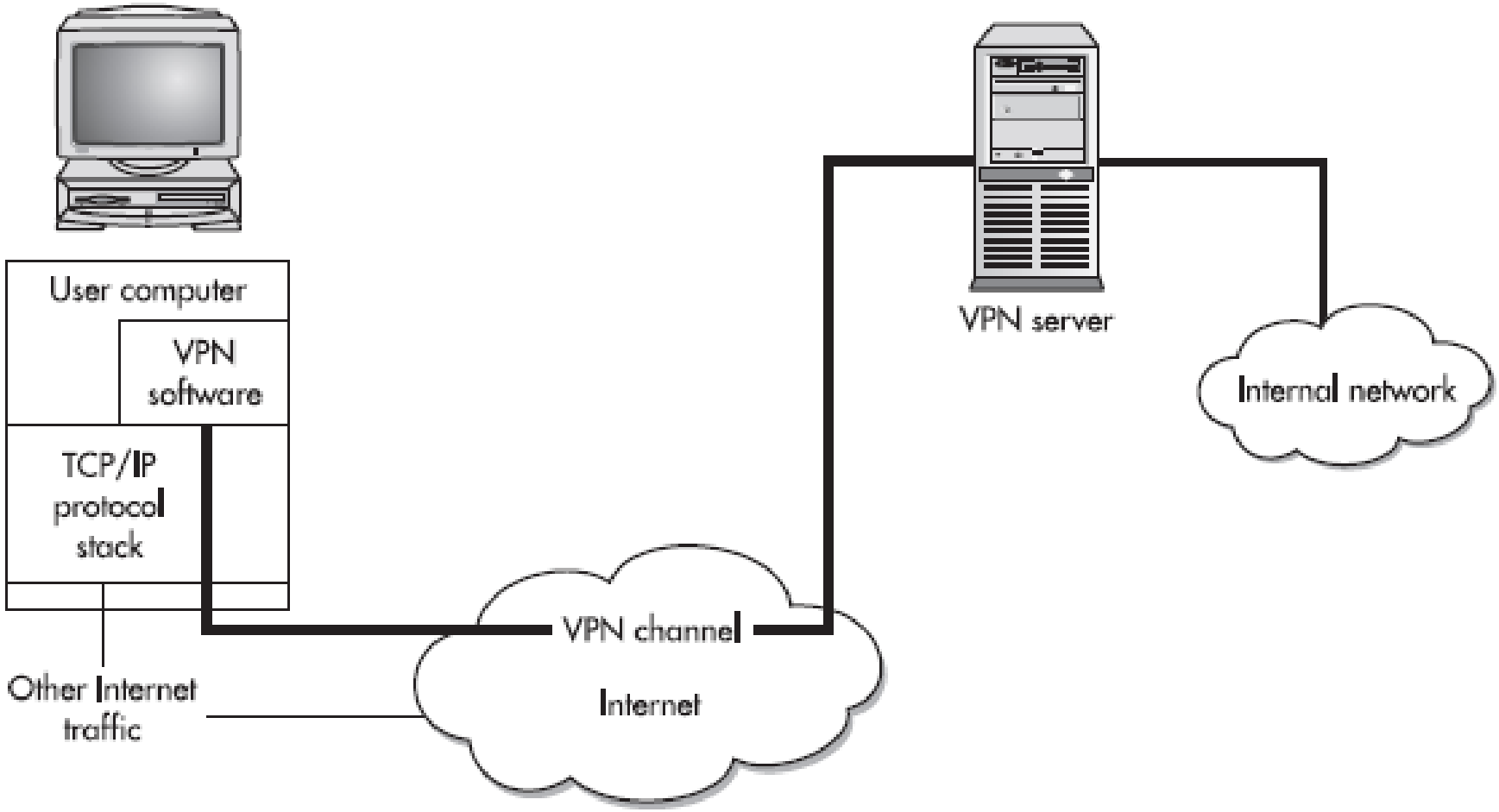
User VPN

- Được dùng nối một máy tính người dùng cá nhân đến một site hay mạng của một tổ chức.
- Thông thường nó được sử dụng cho nhân viên đi du lịch hoặc làm việc từ nhà.
- Máy chủ VPN(VPN Server) có thể là bức tường lửa của tổ chức hoặc có thể là một máy chủ VPN riêng biệt.
- Người sử dụng kết nối với Internet thông qua một ISP cục bộ bằng dial-up, DSL và khởi tạo một kết nối VPN thông qua Internet.

User VPN

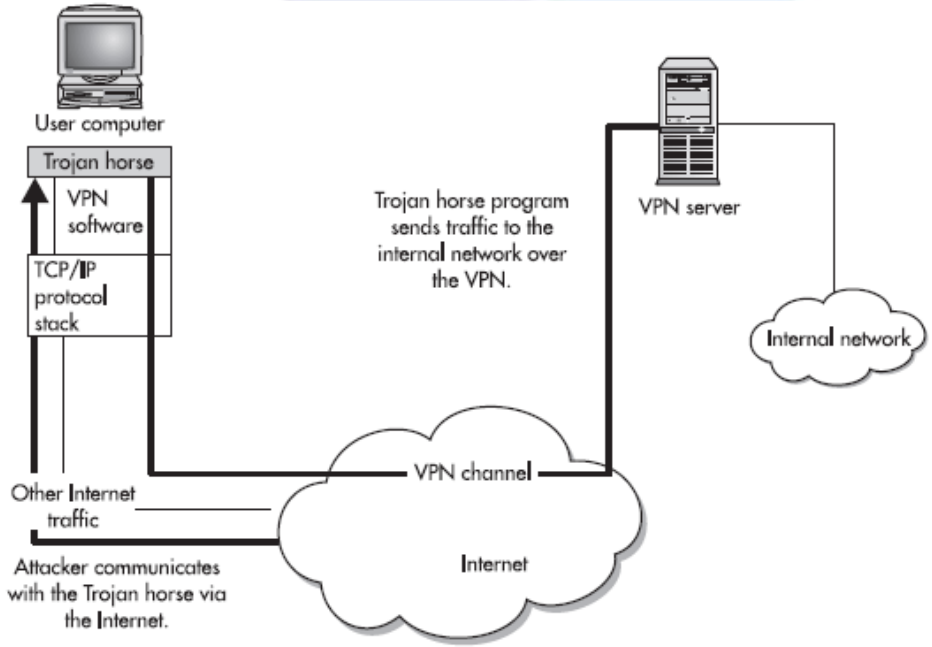
- VPN Sever yêu cầu người dùng xác thực và nếu thành công thì VPN Server cho phép người sử dụng truy cập vào mạng nội bộ của tổ chức.
- Tốc độ mạng sẽ chậm hơn vì các yếu tố hạn chế do người dùng sử dụng kết nối Internet.
- User VPN có thể cho phép các tổ chức hạn chế các hệ thống máy tính hoặc hệ thống tập tin mà người dùng từ xa được phép truy cập. Sự hạn chế này dựa trên chính sách tổ chức và phụ thuộc vào khả năng của sản phẩm VPN.
- User VPN được xử lý bởi một ứng dụng riêng biệt trên máy tính của người dùng.

User VPN


User computer
VPN software
TCP/IP protocol stack
Other Internet traffic
VPN channel
Internet
VPN server
Internal network

Các vấn đề của User VPN

- **Nguy cơ vi phạm an toàn** khá lớn khi người dùng kết nối đồng thời đến các trang Web khác hay thỏa hiệp với một chương trình virus/trojan/worm.



Các vấn đề của User VPN

- **Vấn đề xác thực người dùng**
  - Phải dùng hai yếu tố để xác thực
  - Một yếu tố phải bên ngoài máy tính người dùng
- **Vấn đề tải trên mạng**
  - Số kết nối đồng thời dự kiến phải được thiết lập sao cho độ trễ gây ra do giải mã/mã hóa là không lớn
- **Vấn đề liên quan đến việc sử dụng NAT**
  - Có thể không thực hiện được kết nối VPN khi máy tính ở sau một bức tường lửa và đã được NAT động

Quản lý User VPN

- Quản lý người dùng và các hệ thống máy tính người dùng VPN.
- Có nhiều phiên bản VPN và cấu hình phù hợp cho nhiều hệ điều hành và các yêu cầu khác nhau của các ISP.
- Không nên quên cài đặt một phần mềm anti-virus trên máy tính của người dùng. Nó phải được cập nhật thường xuyên(tốt nhất là hàng tháng).

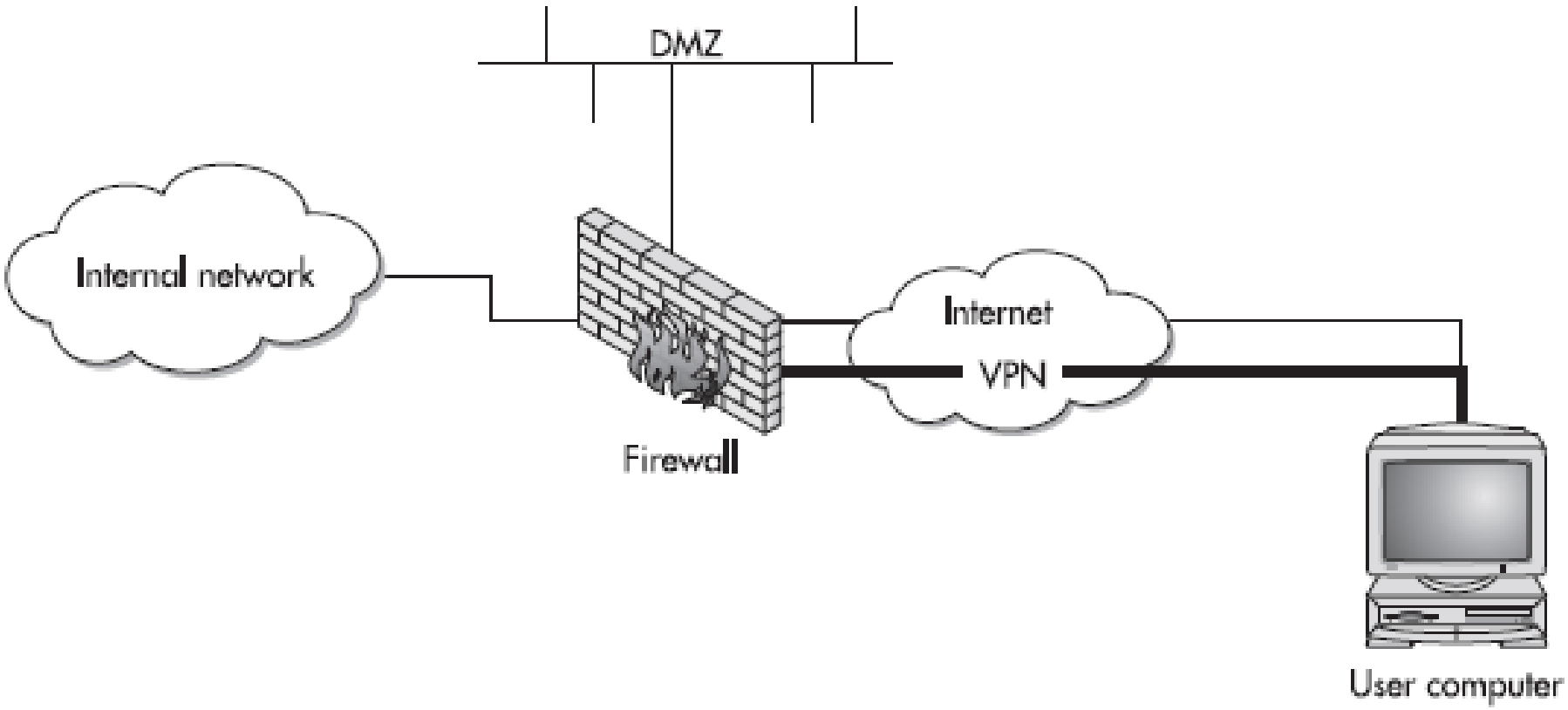
Các thành phần chính của VPN

- VPN server
- Các thuật toán mã hóa
- Hệ thống xác thực
- Giao thức VPN

VPN Server

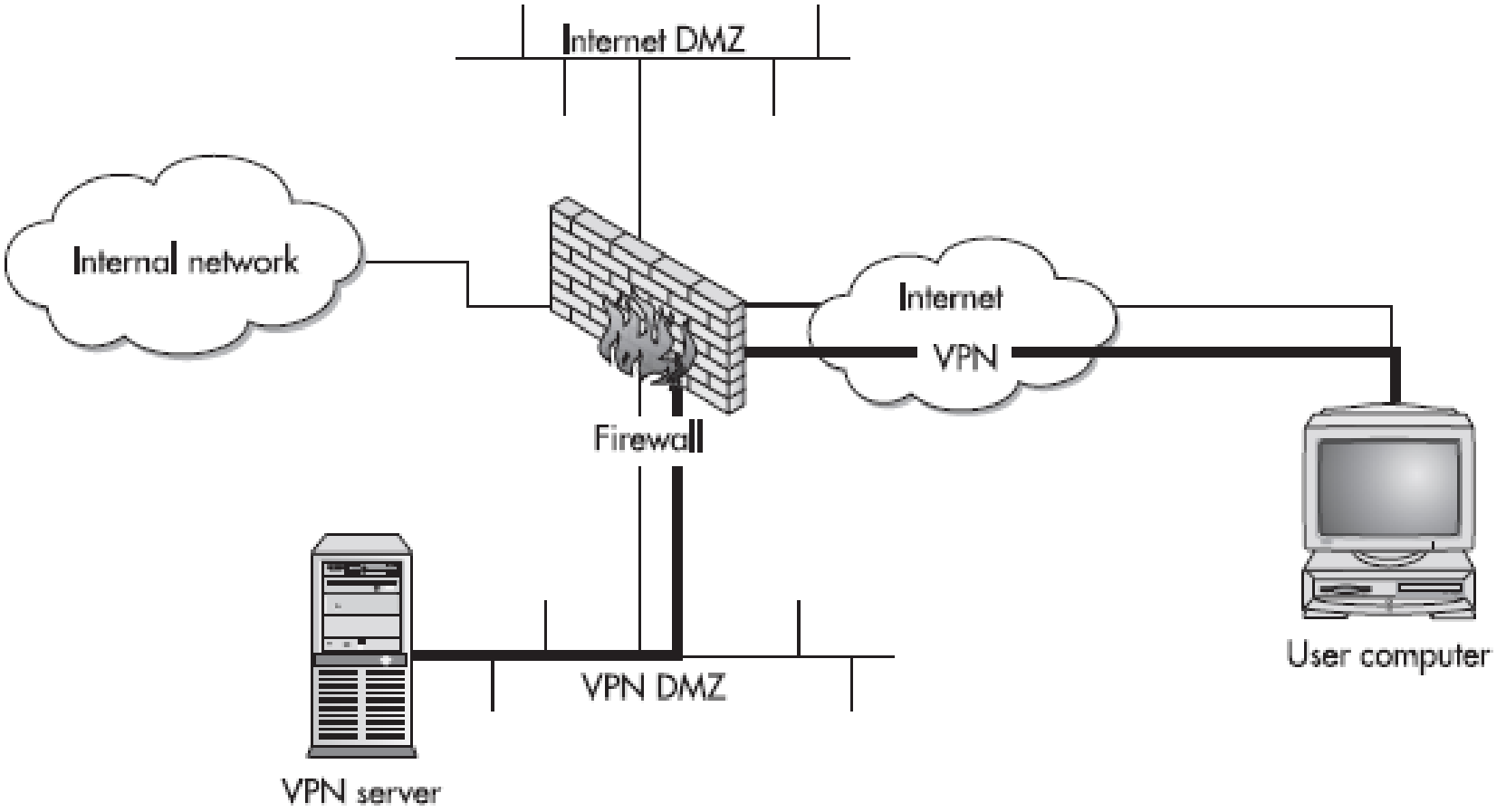
- Hệ thống máy tính hoạt động như một end point cho VPN.
- Một số nhà cung cấp phần mềm VPN Server đề nghị tốc độ bộ xử lý và cấu hình bộ nhớ phụ thuộc vào số lượng VPN kết nối đồng thời.
- Một số VPN Server hỗ trợ fail-over và redundant.
- VPN Server có thể là bức tường lửa hay bộ định tuyến biên.
- VPN Server cũng có thể là một hệ thống độc lập.

VPN Server



Appropriate VPN network architecture when the firewall is the VPN server

VPN Server



Appropriate VPN network architecture for a stand-alone VPN server

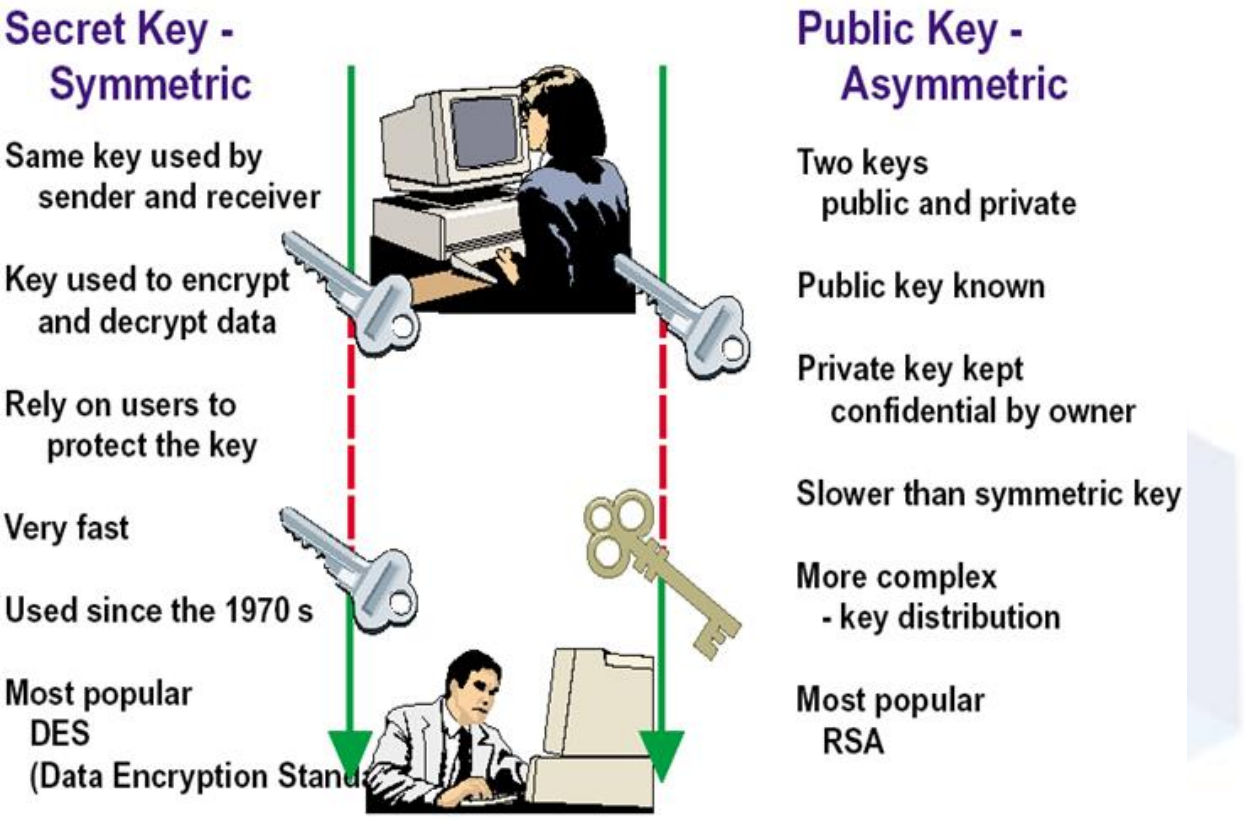
VPN Server

- **Một số quy tắc cần bổ sung trên Firewall**

STT	Nguồn	Đích	Dịch vụ	Hành động
1	Bất kỳ	VPN Server	VPN	Chấp nhận
2	VPN Server	Mạng nội bộ	Bất kỳ	Chấp nhận
3	Bất kỳ	VPN Server	Bất kỳ	Từ chối

Các thuật toán mã hóa

- Các thuật toán sử dụng trong VPN phải là các thuật toán nổi tiếng và mã hóa mạnh.



Hệ thống xác thực

- Phải là hệ thống xác thực trên hai yếu tố.
- Người dùng được xác thực dùng smart card và PIN hay mật khẩu.
- Nếu chỉ dựa vào mật khẩu thì nó phải là mật khẩu mạnh (tối thiểu là tám ký tự và hỗn hợp của các chữ cái, số, và ký tự đặc biệt) và được thay đổi thường xuyên (30 ngày/1 lần).

Giao thức VPN

- Theo nguyên tắc chung nên sử dụng các giao thức chuẩn hơn là giao thức độc quyền.
- Giao thức chuẩn hiện hành đối với mạng riêng ảo là giao thức IPSec.
- Giao thức này là một sự bổ sung để IP đóng gói và mã hóa header và payload các gói tin TCP.
- IPSec cũng xử lý trao đổi khóa, xác thực site từ xa và đàm phán các thuật toán sử dụng.
- Thay thế cho IPSec là SSL. Tuy nhiên SSL được xây dựng để làm việc ở tầng ứng dụng, nó không hiệu quả như IPSec.

Các loại trang thiết bị hỗ trợ VPN

- Phần cứng
- Bức tường lửa
- Phần mềm

Hiện thực dùng phần cứng

- **Dùng bộ định tuyến hỗ trợ VPN**

Ưu điểm	**Nhược điểm**
Khả năng truyền thông cao	Giá thành cao
Tính năng *plug and play*	Tính linh động không cao
Hai mục đích	

Hiện thực dùng bức tường lửa

- **Bảo mật hơn**

Ưu điểm	Khuyết điểm
Hệ điều hành "cứng" hóa. Ba mục đích firewall + router + VPN Đầu tư khá hiệu quả	Chi phí khá lớn

Hiện thực dùng phần mềm

- **Được dùng khi hai đầu cuối không cùng một tổ chức.**

Ưu điểm
Tính linh động cao
Chi phí thấp

Khuyết điểm
Hiệu quả thấp
Đòi hỏi cần đào tạo
Chi phí sản phẩm thấp nhưng chi phí cấu hình cao hơn.

Tóm tắt

- VPN là một loại mạng riêng sử dụng môi trường truyền thông công cộng như Internet, thay vì dùng đường thuê bao (leased line) để truyền thông
- VPN bao gồm hai loại là Site to Site VPN và User VPN.
- Các thành phần chính của VPN là VPN Server, thuật toán mã hóa, hệ thống xác thực và giao thức VPN như IPSec, SSL, ..
- Có nhiều loại trang thiết bị hỗ trợ VPN như bộ định tuyến, bức tường lửa hoặc sử dụng phần mềm.