ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CNTT&TT

PHẠM VĂN ĐOAN

NGHIÊN CỨU MẠNG RIÊNG ẢO VÀ ỨNG DỤNG TRONG THƯƠNG MẠI ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, NĂM 2012

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CNTT&TT

PHẠM VĂN ĐOAN

NGHIÊN CỨU MẠNG RIÊNG ẢO VÀ ỨNG DỤNG TRONG THƯƠNG MẠI ĐIỆN TỬ

Chuyên ngành : **Khoa học máy tính**
Mã số : **60.48.01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS.TS TRỊNH NHẬT TIẾN

THÁI NGUYÊN, NĂM 2012

MỞ ĐẦU

Với sự phát triển nhanh chóng của công nghệ thông tin và viễn thông, thế giới ngày càng thu nhỏ và trở nên gần gũi. Nhiều công ty đang vượt qua ranh giới cục bộ và khu vực, vươn ra thị trường thế giới. Nhiều doanh nghiệp có tổ chức trải rộng khắp toàn quốc thậm chí vòng quanh thế giới, và tất cả họ đều đối mặt với một nhu cầu thiết thực: một cách thức nhằm duy trì những kết nối thông tin kịp thời, an toàn và hiệu quả cho dù văn phòng đặt tại bất cứ nơi đâu.

Bên cạnh đó các hoạt động giao dịch thương mại đã không còn chỉ là các giao dịch truyền thống, mà thay vào đó, một xu thế đang phát triển mạnh mẽ và phù hợp thời đại là các giao dịch thương mại điện tử. Sự phát triển mạnh mẽ của thương mại điện tử sẽ mang đến cho xã hội một tiện ích vô cùng to lơn, khi đó các giao dịch sẽ diễn ra nhanh chóng, kịp thời và phù hợp trong khi người dùng chỉ cần ngồi ngay tại nhà mình.

Tuy nhiên các giao dịch thương mại điện tử chỉ có thể gọi là thành công nếu nó đảm bảo được tính an toàn cho các giao dịch, nhất là các giao dịch này lại diễn ra trên môi trường internet – là môi trường luôn luôn tiềm ẩn rất nhiều nguy cơ mất an toàn dữ liệu. Từ đây, ta thấy song song với việc phát triển của thương mại điện tử thì cần phải nghiên cứu giải quyết vấn đề an toàn thông tin trong mỗi giao dịch.

Nhận ra yêu cầu đó cùng với sự gợi ý của giáo viên hướng dẫn và dựa trên những tìm hiểu của em, em chọn đề tài nghiên cứu "**Nghiên cứu mạng riêng ảo và ứng dụng trong thương mại điện tử".**

Với mục đích nghiên cứu về công nghệ mạng riêng ảo, đề từ đó ứng dụng vào thương mại điện tử, tạo hành lang an toàn cho các giao dịch thương mại điện tử luận văn sẽ gồm 3 chương cụ thể như sau:

Chương 1: Khái quát về mạng riêng ảo và thương mại điện tử

Chương 2: Một số vấn đề về an toàn thông tin trong bài toán thỏa thuận ký kết hợp đồng điện tử.

Chương 3: Chương trình thực nghiệm

Do hạn chế về nhiều mặt nên Luận văn chắc chắn không tránh khỏi những thiếu xót, rất mong được sự đóng góp ý kiến của Thầy, Cô và các bạn để Luận văn được hoàn thiện hơn.

Em xin chân thành cảm ơn thầy giáo, PGS. TS Trịnh Nhật Tiến đã tận tình hướng dẫn và giúp đỡ em trong suốt quá trình hoàn thành luận văn. Em cũng xin trân thành cảm ơn các thầy, cô, bạn bè cùng toàn thể người thân đã giúp đỡ và chỉ bảo cho em trong thời gian thực hiện luận văn này.

Chương 1
KHÁI QUÁT VỀ MẠNG RIÊNG ẢO VÀ THƯƠNG MẠI ĐIỆN TỬ

1.1. KHÁI QUÁT VỀ MẠNG RIÊNG ẢO

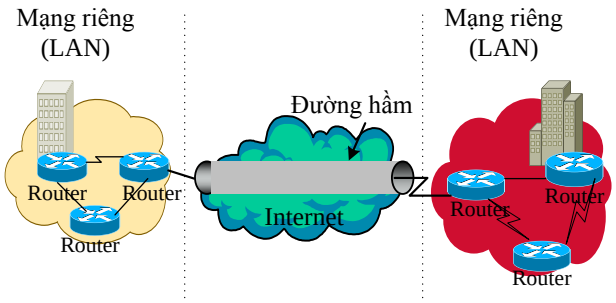
1.1.1. Khái niệm mạng riêng ảo

Cụm từ Virtual Private Network (mạng riêng ảo) thường được gọi tắt là VPN là một kỹ thuật đã xuất hiện từ lâu, tuy nhiên nó thực sự bùng nổ và trở nên cạnh tranh khi xuất hiện công nghệ mạng thông minh với đà phát triển mạnh mẽ của Internet. Trong thực tế, người ta thường nói tới hai khái niệm VPN đó là: mạng riêng ảo kiểu tin tưởng (Trusted VPN) và mạng riêng ảo an toàn (Secure VPN).

Mạng riêng ảo kiểu tin tưởng được xem như một số mạch thuê của một nhà cung cấp dịch vụ viễn thông. Mỗi mạch thuê riêng hoạt động như một đường dây trong một mạng cục bộ. Tính riêng tư của trusted VPN thể hiện ở chỗ nhà cung cấp dịch vụ sẽ đảm bảo không có một ai sử dụng cùng mạch thuê riêng đó. Các mạng riêng xây dựng trên các đường dây thuê thuộc dạng "trusted VPN".

Mạng riêng ảo an toàn là các mạng riêng ảo có sử dụng mật mã để bảo mật dữ liệu. Dữ liệu ở đầu ra của một mạng được mật mã rồi chuyển vào mạng công cộng (ví dụ: mạng Internet) như các dữ liệu khác để truyền tới đích và sau đó được giải mã dữ liệu tại phía thu. Dữ liệu đã mật mã có thể coi như được truyền trong một đường hầm (tunnel) bảo mật từ nguồn tới đích. Cho dù một kẻ tấn công có thể nhìn thấy dữ liệu đó trên đường truyền thì cũng không có khả năng đọc được vì dữ liệu đã được mật mã.

Mạng riêng ảo VPN được định nghĩa là một kết nối mạng triển khai trên cơ sở hạ tầng mạng công cộng (như mạng Internet) với các chính sách quản lý và bảo mật giống như mạng cục bộ.



Hình 1.1: Mô hình mạng riêng ảo.

a) Chức năng

VPN cung cấp ba chức năng chính đó là: tính xác thực (Authentication), tính toàn vẹn (Integrity) và tính bảo mật (Confidentiality).

Tính xác thực : Để thiết lập một kết nối VPN thì trước hết cả hai phía phải xác thực lẫn nhau để khẳng định rằng mình đang trao đổi thông tin với người mình mong muốn chứ không phải là một người khác.

Tính toàn vẹn : Đảm bảo dữ liệu không bị thay đổi hay đảm bảo không có bất kỳ sự xáo trộn nào trong quá trình truyền dẫn.

Tính bảo mật : Người gửi có thể mã hoá các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở phía thu. Bằng cách làm như vậy, không một ai có thể truy nhập thông tin mà không được phép. Thậm chí nếu có lấy được thì cũng không đọc được.

b) Ưu điểm

VPN mang lại lợi ích thực sự và tức thời cho các công ty, tổ chức. Có thể dùng VPN không chỉ để đơn giản hoá việc thông tin giữa các nhân viên làm việc ở xa, người dùng lưu động, mở rộng Intranet đến từng văn phòng, chi nhánh, thậm chí triển khai Extranet đến tận khách hàng và các đối tác chủ chốt mà còn làm giảm chi phí cho công việc trên thấp hơn nhiều so với việc mua thiết bị và đường dây cho mạng WAN riêng. Những lợi ích này dù trực tiếp hay gián tiếp đều bao gồm: Tiết kiệm chi phí (cost saving), tính mềm dẻo (flexibility), khả năng mở rộng (scalability) và một số ưu điểm khác

1.1.2. Phân loại mạng riêng ảo

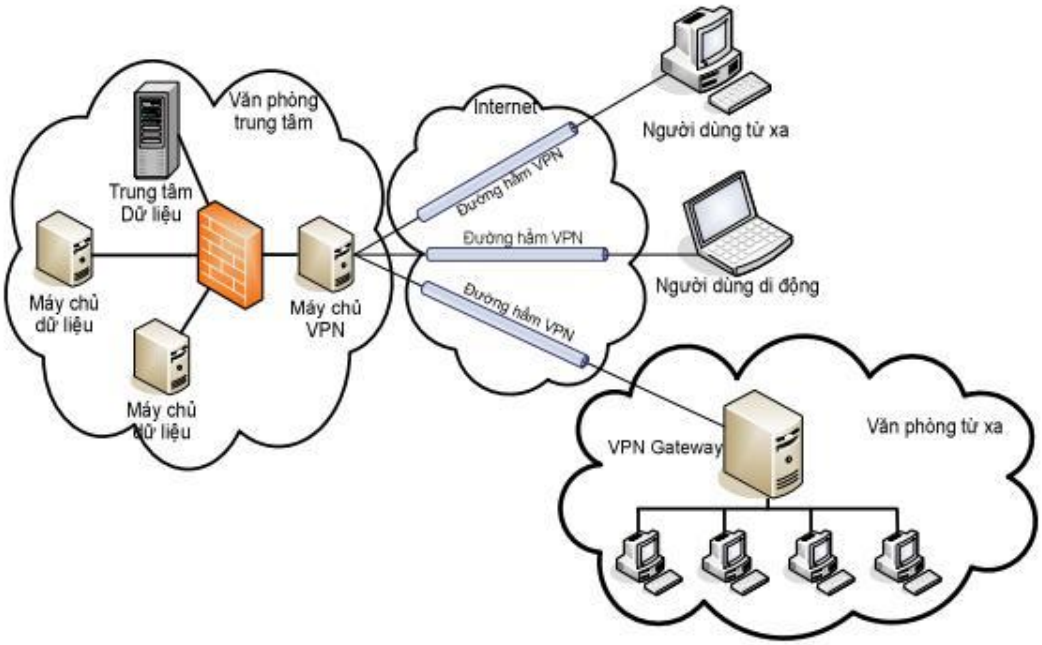
Dựa vào những yêu cầu cơ bản mạng riêng ảo được phân làm ba loại:

- VPN truy nhập từ xa (Remote Access VPNs)
- VPN Site – To – Site:
  - Mạng VPN cục bộ (Intranet VPN)
  - Mạng VPN mở rộng (Extranet VPN)

a) VPN truy nhập từ xa (Remote access VPNs)

VPN truy nhập từ xa cung cấp cho các nhân viên, chi nhánh văn phòng di động có khả năng trao đổi, truy nhập từ xa vào mạng của công ty tại mọi thời điểm tại bất cứ đâu có mạng Internet.

VPN truy nhập từ xa cho phép mở rộng mạng công ty tới những người sử dụng thông qua cơ sở hạ tầng chia sẻ chung, trong khi những chính sách mạng công ty vẫn duy trì. Loại VPN này có thể dùng để cung cấp truy nhập an toàn cho các thiết bị di động, những người sử dụng di động, các chi nhánh và những bạn hàng của công ty. Những kiểu VPN này được thực hiện thông qua cơ sở hạ tầng công cộng bằng cách sử dụng công nghệ ISDN, quay số, IP di động, DSL và công nghệ cáp và thường yêu cầu một vài kiểu phần mềm client chạy trên máy tính của người sử dụng.



Hình 1.2: VPN truy nhập từ xa.

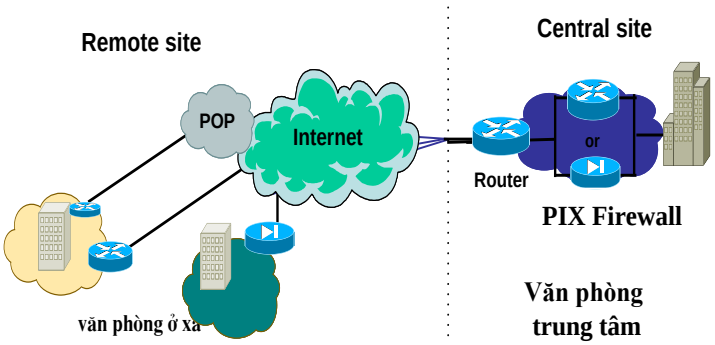
b) VPN Site To Site

Site-to-Site VPN được sử dụng để nối các site của các hãng phân tán về mặt địa lý, trong đó mỗi site có các địa chỉ mạng riêng được quản lý sao cho bình thường không xảy ra va chạm.

Mạng VPN cục bộ (Intranet VPN)

Các VPN cục bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty. Mạng VPN liên kết trụ sở chính, các văn phòng, chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối luôn được mã hoá bảo mật. Điều này cho phép tất cả các địa điểm có thể truy nhập an toàn các nguồn dữ liệu được phép trong toàn bộ mạng của công ty.

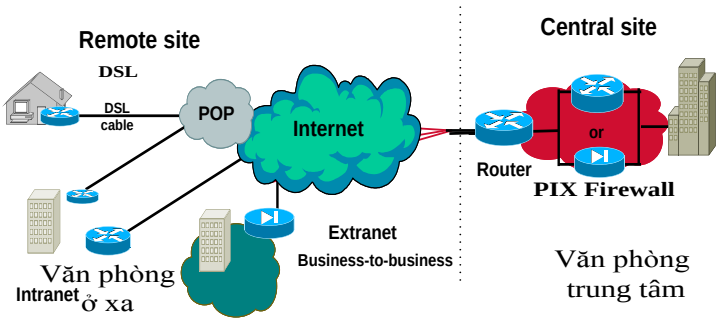
Những VPN này vẫn cung cấp những đặc tính của mạng WAN như khả năng mở rộng, tính tin cậy và hỗ trợ cho nhiều kiểu giao thức khác nhau với chi phí thấp nhưng vẫn đảm bảo tính mềm dẻo. Kiểu VPN này thường được cấu hình như là một VPN Site- to- Site.



Hình 1.3: VPN cục bộ.

Mạng VPN mở rộng (Extranet VPN)

Không giống như mạng VPN cục bộ và mạng VPN truy nhập từ xa, mạng VPN mở rộng không bị cô lập với "thế giới bên ngoài". Thực tế mạng VPN mở rộng cung cấp khả năng điều khiển truy nhập tới những nguồn tài nguyên mạng cần thiết để mở rộng những đối tượng kinh doanh như là các đối tác, khách hàng, và các nhà cung cấp…



Hình 1.4: VPN mở rộng.

Các VPN mở rộng cung cấp một đường hầm bảo mật giữa các khách hàng, các nhà cung cấp và các đối tác qua một cơ sở hạ tầng công cộng. Kiểu VPN này sử dụng các kết nối luôn luôn được bảo mật và được cấu hình như một VPN Site–to–Site. Sự khác nhau giữa một VPN cục bộ và một VPN mở rộng đó là sự truy cập mạng được công nhận ở một trong hai đầu cuối của VPN.

1.1.3. Các giáo thức đường hầm trong mạng riêng ảo

a) Giao thức định hướng L2F (Layer 2 Forwarding).

Giao thức định hướng lớp 2 L2F do Cisco phát triển độc lập và được phát triển dựa trên giao thức PPP (Point-to-Point Protocol). L2F cung cấp giải pháp cho dịch vụ quay số ảo bằng cách thiết lập một đường hầm bảo mật thông qua cơ sở hạ tầng công cộng như Internet. L2F là giao thức được phát triển sớm nhất, là phương pháp truyền thống để cho những người sử dụng ở xa truy cập vào một mạng công ty thông qua thiết bị truy cập từ xa. L2F cho phép đóng gói các gói PPP trong L2F, định đường hầm ở lớp liên kết dữ liệu.

Ưu nhược điểm của L2F

Ưu điểm:

- Cho phép thiết lập đường hầm đa giao thức.
- Được cung cấp bởi nhiều nhà cung cấp.

Nhược điểm:

- Không có mã hoá.
- Yếu trong việc xác thực người dùng.
- Không có điều khiển luồng cho đường hầm.

Hoạt động của L2F

Hoạt động L2F bao gồm các hoạt động: thiết lập kết nối, đường hầm và phiên làm việc. Ta xem xét ví dụ minh hoạ hoạt động của L2F:

1) Một người sử dụng ở xa quay số tới hệ thống NAS và khởi đầu một kết nối PPP tới ISP.
2) Hệ thống NAS và máy khách trao đổi các gói giao thức điều khiển liên kết LCP (Link Control Protocol).

3) NAS sử dụng cơ sở dữ liệu cục bộ liên quan tới tên vùng (domain name) hay nhận thực RADIUS để quyết định có hay không người sử dụng yêu cầu dịch vụ L2F.
4) Nếu người sử dụng yêu cầu L2F thì quá trình tiếp tục: NAS thu nhận địa chỉ của gateway đích (home gateway).
5) Một đường hầm được thiết lập từ NAS tới gateway đích nếu giữa chúng chưa có đường hầm nào. Sự thành lập đường hầm bao gồm giai đoạn nhận thực từ ISP tới gateway đích để chống lại tấn công bởi những kẻ thứ ba.
6) Một kết nối PPP mới được tạo ra trong đường hầm, điều này tác động kéo dài phiên PPP từ người sử dụng ở xa tới home gateway. Kết nối này được thiết lập như sau: Home gateway tiếp nhận các lựa chọn và tất cả thông tin nhận thực PAP/CHAP, như đã thoả thuận bởi đầu cuối người sử dụng và NAS. Home gateway chấp nhận kết nối hay nó thoả thuận lại LCP và nhận thực lại người sử dụng.
7) Khi NAS tiếp nhận lưu lượng dữ liệu từ người sử dụng, nó lấy gói và đóng gói lưu lượng vào trong một khung L2F và hướng nó vào trong đường hầm.
8) Tại home gateway, khung L2F được tách bỏ, và dữ liệu đóng gói được hướng tới mạng công ty.

b) Giao thức PPTP (Point –to- Point Tunneling Protocol)

Giao thức đường hầm điểm–điểm PPTP được đưa ra đầu tiên bởi một nhóm các công ty được gọi là PPTP Forum. Nhóm này bao gồm 3 công ty: Ascend comm., Microsoft, ECI Telematicsunication và US Robotic. Ý tưởng cơ sở của giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa người dùng ở xa (client) và mạng riêng. Người dùng ở xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo đường hầm bảo mật tới mạng riêng của họ.

Giao thức PPTP được xây dựng dựa trên chức năng của PPP, cung cấp khả năng quay số truy cập tạo ra một đường hầm bảo mật thông qua Internet đến site đích. PPTP sử dụng giao thức bọc gói định tuyến chung GRE (Generic Routing