

TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THÔNG TIN

HỮU NGHỊ VIỆT-HÀN

KHOA KHOA HỌC MÁY TÍNH

— □□□ —

ĐỒ ÁN CHUYÊN ĐỀ
NGÀNH MẠNG MÁY TÍNH

ĐỀ TÀI
NGHIÊN CỨU VÀ TRIỂN KHAI OPENVPN
TRÊN UBUNTU CHO DOANH NGHIỆP

SVTH: Lê Long Bảo

Lớp : MM03A

Niên khóa : 2009 – 2012

CBHD : Thạc sĩ Đặng Quang Hiễn

Đà Nẵng, tháng 3 năm 2012

LỜI CẢM ƠN

Để hoàn thành đồ án chuyên đề này, lời đầu tiên em xin chân thành cảm ơn các thầy giáo, cô giáo Khoa Khoa học máy tính, những người đã dạy dỗ, trang bị cho em những kiến thức bổ ích trong năm học vừa qua.

Em xin bày tỏ lòng biết ơn sâu sắc nhất tới thầy Đặng Quang Hiến, người đã tận tình hướng dẫn em trong suốt quá trình làm đồ án

Một lần nữa em xin chân thành cảm ơn sự giúp đỡ của các thầy cô

Đà Nẵng, ngày 15 tháng 3 năm 2012

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Ý nghĩa
VPN	Virtual Private Network
GNU	General Public License

FSF	Free Software Foundation
GCC	GNU C Compiler
PMMNM	Phần mềm mã nguồn mở
GPL	General Public License
DLL	Dynamic Link Library
WAN	Wire Area Network
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
PPTP	Point-to-Point Tunneling Protocol
GRE	Generic Routing Encapsulation

DANH MỤC HÌNH VẼ

LỜI MỞ ĐẦU

Hiện nay, Internet đã phát triển mạnh mẽ cả về mặt mô hình lẫn tổ chức, đáp ứng khá đầy đủ các nhu cầu của người sử dụng. Internet đã được thiết kế để kết nối nhiều mạng với nhau và cho phép thông tin chuyển đến người sử dụng một cách tự do và nhanh chóng. Để làm được điều này người ta sử dụng một hệ thống các thiết bị định tuyến để kết nối các LAN và WAN với nhau. Các máy tính được kết nối vào Internet thông qua các nhà cung cấp dịch vụ ISP. Với Internet, những dịch vụ như đào tạo từ xa, mua hàng trực tuyến, tư vấn các lĩnh vực và rất nhiều điều khác đã trở thành hiện thực. Tuy nhiên do Internet có phạm vi toàn cầu và không một tổ chức, chính phủ cụ thể nào quản lý nên rất khó khăn trong việc bảo mật và an toàn dữ liệu, cũng như việc quản lý dịch vụ.

Các doanh nghiệp có chuỗi chi nhánh, cửa hàng ngày càng trở nên phổ biến. Không những vậy, nhiều doanh nghiệp còn triển khai đội ngũ bán hàng đến tận người dùng. Do đó, để kiểm soát, quản lý, tận dụng tốt nguồn tài nguyên, nhiều doanh nghiệp đã triển khai giải pháp phần mềm quản lý nguồn tài nguyên có khả năng hỗ trợ truy cập, truy xuất thông tin từ xa. Tuy nhiên, việc truy xuất cơ sở dữ liệu từ xa luôn đòi hỏi cao về vấn đề an toàn, bảo mật.

Để giải quyết vấn đề trên, nhiều doanh nghiệp đã chọn giải pháp mô hình mạng riêng ảo VPN (Virtual Private Network). Với mô hình mới này, người ta không phải đầu tư thêm nhiều về cơ sở hạ tầng mà các tính năng như bảo mật và độ tin cậy vẫn được bảo đảm, đồng thời có thể quản lý riêng sự hoạt động của mạng này. VPN cho phép người sử dụng làm việc tại nhà riêng, trên đường đi, hoặc các văn phòng chi nhánh có thể kết nối an toàn tới máy chủ của tổ chức mình bằng cơ sở hạ tầng được cung cấp bởi mạng công cộng. Nhưng thông thường, triển khai phần mềm VPN và phần cứng tốn nhiều thời gian và chi phí, do đó OpenVPN là một giải pháp mã nguồn mở VPN hoàn toàn miễn phí.

Nội dung đề án được trình bày trong 3 chương

Chương 1 : Tổng quan về phần mềm nguồn mở

Chương 2 : Công nghệ VPN và các giao thức hỗ trợ

Chương 3 : Mô hình hệ thống và triển khai OpenVPN trên Ubuntu Server

Tiếp theo là phần kết luận và cuối cùng là tài liệu tham khảo.

CHƯƠNG 1 : TỔNG QUAN VỀ PHẦN MỀM NGUỒN MỞ

1.1. GIỚI THIỆU PHẦN MỀM MÃ NGUỒN MỞ VÀ HỆ ĐIỀU HÀNH LINUX

1.1.1. Khái niệm phần mềm mã nguồn mở

1.1.1.1. Lịch sử phát triển phần mềm mã nguồn mở

Việc sử dụng hệ điều hành UNIX và các công cụ hỗ trợ đi kèm đã khiến cho các nhà phát triển phần mềm cảm thấy bản quyền hạn chế sự sáng tạo của họ. Năm 1983, dự án GNU ra đời, do Richard Stallman sáng lập. Dự án này phát triển thành Tổ chức phần mềm tự do FSF (Free Software Foundation). Tổ chức này tập hợp các nhà phát triển thường xuyên sử dụng UNIX, hướng tới mục tiêu là phát triển các công cụ tương tự như của UNIX nhưng hoàn toàn tự do và mã nguồn mở. GCC (GNU C Compiler) là sản phẩm đầu tiên, cho phép phát triển các sản phẩm khác, vì là chương trình soạn thảo thông dụng, ...và các sản phẩm khác

Năm 1988 các nỗ lực ủng hộ PMMN (Phần mềm mã nguồn mở) đã hình thành OSI (Open Source Initiative). OSI nỗ lực để tạo ra các khung pháp lý, cung cấp các thông tin cần thiết cho người sử dụng, các nhà phát triển, các công ty dịch vụ có thể phát triển, khai thác, cung cấp dịch vụ, kinh doanh PMMN

Mặc dù có một quá trình phát triển khá lâu dài, tuy nhiên trên thực tế phải đến năm 2008 mới có những quy định chặt chẽ của pháp luật, một số nước bảo hộ PMMN. Ví dụ khi bạn vi phạm bản quyền của phần mềm, tất cả các quyền được gán trong bản quyền lập tức trở thành vô hiệu. Quy định này không tác động nhiều đến phần mềm sở hữu, nhưng với PMMN, khi các quyền trở thành vô hiệu hầu như chắc chắn người sử dụng sẽ vi phạm các sở hữu trí tuệ.

1.1.1.2. Định nghĩa phần mềm nguồn mở

Để hiểu được phần mềm mã nguồn mở là gì, đầu tiên chúng ta phải hiểu phần mềm là gì, mã nguồn mở là gì, và phần mềm mã nguồn mở là gì.

Phần mềm hiểu theo nghĩa đen là một tập hợp các câu lệnh, được viết bằng một hoặc nhiều ngôn ngữ lập trình theo một trật tự xác định, nhằm tự động thực hiện một số chức năng hoặc giải quyết một bài toán nào đó. Hiểu theo nghĩa bóng thì phần mềm là một sản phẩm đặc biệt, đặc trưng cho ngành Công nghệ thông tin và Công nghệ phần mềm.

Mã nguồn mở, tên tiếng anh là Open Source, là thuật ngữ chỉ các phần mềm công khai mã nguồn. Người dùng không phải trả một khoản chi phí nào, hơn thế nữa họ có quyền xem, sửa đổi và cải tiến, nâng cấp theo một số nguyên tắc chung quy định trong giấy phép phần mềm nguồn mở GPL (General Public License). Ông tổ của mã nguồn mở là Richard Stallman, người đã xây dựng dự án GNU, và cho ra giấy phép mã nguồn mở GPL, hai nền tảng then chốt cho sự phát triển của mã nguồn mở.

Từ hai định nghĩa trên ta có thể hiểu được, phần mềm nguồn mở là gì. Phần mềm nguồn mở là phần mềm được cung cấp dưới dạng mã và nguồn, không chỉ miễn phí về giá mua mà chủ yếu là miễn phí về bản quyền. Người dùng có quyền sửa đổi, cải tiến, phát triển, nâng cấp theo một số nguyên tắc chung quy định trong giấy phép Phần mềm nguồn mở (ví dụ như GPL – General Public License) mà không cần xin phép ai, điều mà họ không được phép làm với phần mềm nguồn đóng (tức là phần mềm thương mại).

1.1.1.3. Các thao tác trên phần mềm mã nguồn mở

Trên phần mềm, có thể thực hiện các thao tác:

Sản xuất phần mềm: Nghiên cứu nhu cầu của người sử dụng, thiết kế, coding, compiling và releasing

Cài đặt phần mềm: Để có thể sử dụng, phần mềm cần được cài đặt. Cài đặt là thao tác ghi các mã cần thiết cho việc thực hiện môi trường vào bộ nhớ thích hợp để người sử dụng có thể sử dụng

Sử dụng phần mềm: Cài đặt và sử dụng phần mềm trên máy tính. Máy tính này có thể là máy tính cá nhân, máy chủ, máy tính công cộng,...Tùy theo từng bối cảnh việc sử dụng phần mềm có thể có các ràng buộc khác nhau (cài trên một máy, cài trên nhiều máy, cài trên nhiều CPU,...). Các phần mềm có bản quyền thường bảo vệ việc sử dụng phần mềm bằng serial key, active code và có những trường hợp bằng khóa vật lý.

Thay đổi phần mềm: Trong quá trình sử dụng có thể xuất hiện nhu cầu thay đổi. Việc thay đổi này có thể được tiến hành bởi nhà tác giả sản xuất phần mềm, hoặc có thể do một người khác. Để thay đổi tính năng phần mềm cần có mã nguồn của phần mềm. Nếu không có mã nguồn có thể dịch ngược để thu mã nguồn từ mã thực hiện. Mã nguồn phần mềm có thể được phân phối theo nhiều kênh khác nhau (mạng, lưu trữ, truyền tay, lây nhiễm).

Các thao tác khác: Phân tích ngược mã nguồn, phân tích giao diện, mô phỏng, thực hiện luân phiên,...Phần mềm được quản lý bởi các quy tắc về bản quyền và sở hữu trí tuệ, cho phép thực hiện hoặc không thực hiện các thao tác nói trên trong các điều kiện khác nhau.

Bản quyền phần mềm: Là tài liệu quy định việc thực hiện các thao tác trên phần mềm. Có thể có các bản quyền phần mềm sở hữu, bản quyền cho phần mềm miễn phí / phần mềm chia sẻ, bản quyền cho phần mềm tự do và mã nguồn mở.

1.1.2. Giới thiệu hệ điều hành Linux

1.1.2.1. Lịch sử Linux

Linux là hệ điều hành mô phỏng Unix, được xây dựng trên phần nhân (kernel), và gói phần mềm mã nguồn mở. Linux được công bố dưới bản quyền của GPL (General Public License).

Unix ra đời giữa những năm 1960, ban đầu được phát triển bởi AT&T, sau đó được đăng ký thương mại và phát triển theo nhiều dòng dưới cái tên khác nhau. Năm 1990 xu hướng phát triển phần mềm nguồn mở xuất hiện và được thúc đẩy bởi tổ chức GNU. Một số license về mã nguồn mở ra đời ví dụ BSD, GPL. Năm 1991, Linus Torvald viết thêm phiên bản nhân v0.01 (kernel) đầu tiên của Linux đưa lên các BBS, nhóm người dùng để mọi người cùng sử dụng và phát triển. Năm 1996, nhân v1.0 chính thức công bố và ngày càng nhận được sự quan tâm của người dùng. Năm 1999, phiên bản nhân v2.2 mang nhiều đặc tính ưu việt và giúp cho Linux bắt đầu trở thành đối thủ cạnh tranh đáng kể của MSWindows trên môi trường Server. Năm 2000 phiên bản nhân v2.4 hỗ trợ nhiều thiết bị mới (đa xử lý tới 32 chip, USB, RAM trên 2GB...) bắt đầu đặt chân vào thị trường máy chủ cao cấp. Quá trình phát triển Linux như sau:

- Năm 1991: 100 người dùng.
- Năm 1997: 7.000.000 người dùng.
- Năm 2000: hàng trăm triệu người dùng, hơn 15.000 người tham gia phát triển Linux. Hàng năm thị trường cho Linux tăng trưởng trên 100%.

Các phiên bản Linux là sản phẩm đóng gói kernel và các gói phần mềm miễn phí khác. Các phiên bản này được công bố dưới license GPL. Một số phiên bản nổi bật là: Redhat, Caldera, Suse, Debian, TurboLinux, Mandrake.

Giống như Unix, Linux gồm 3 thành phần chính: kernel, shell và cấu trúc file.

Kernel là chương trình nhân, chạy các chương trình và quản lý các thiết bị phần cứng như đĩa và máy in

Shell (môi trường) cung cấp giao diện cho người sử dụng, còn được mô tả như một bộ biên dịch. Shell nhận các câu lệnh từ người sử dụng, và gửi các câu lệnh đó cho nhân thực hiện. Nhiều shell được phát triển, linux cung cấp một số shell như: desktops, windows manager, và môi trường dòng lệnh. Hiện nay chủ yếu tồn tại 3 shell: Bourne, Korn và C Shell. Bourne được phát triển tại phòng thí nghiệm, Bell và C Shell được phát triển cho phiên bản BSD của Unix, Korn shell là phiên bản cải tiến của Bourne Shell. Những phiên bản hiện nay của Unix, bao gồm cả Linux, tích hợp cả 3 shell trên.

Cấu trúc file quy định cách lưu trữ file trên đĩa. File được nhóm trong các thư mục. Mỗi thư mục có thể chứa file và các thư mục con khác. Một số thư mục là các thư mục chuẩn do hệ thống sử dụng. Người dùng có thể tạo các file/ thư mục của riêng mình cũng như dịch chuyển các file giữa các thư mục đó. Hơn nữa, với Linux người dùng có thể thiết lập quyền truy cập file/ thư mục, cho phép hay hạn chế một người dùng hoặc một nhóm truy cập file. Các thư mục trong Linux được tổ chức theo cấu trúc cây, bắt đầu bằng thư mục gốc (root). Các thư mục khác được phân nhánh từ thư mục này

Kernel, shell và cấu trúc file cấu thành nên cấu trúc hệ điều hành. Với những thành phần trên người dùng có thể chạy chương trình, quản lý file, và tương tác với hệ thống.

1.1.2.2. *Giao tiếp trên môi trường Linux*

Terminal: Khái niệm Terminal xuất hiện từ xa xưa khi các hệ thống máy tính rất lớn, người sử dụng không tương tác trực tiếp với hệ thống mà thông qua các Terminal ở xa. Các hệ thống Terminal này gồm màn hình và bàn phím, ngày nay do kích thước bé đi nên các Terminal này chính là máy tính của người sử dụng.

Console: Ngoài ra hệ thống Linux nói chung hay các máy chủ dịch vụ của các hệ điều hành khác nói riêng đều cung cấp cho người quản trị một giao diện Terminal đặc biệt gọi là Console. Trước kia console tồn tại dưới dạng một cổng giao tiếp riêng biệt,

còn ngày nay dưới dạng một Console ảo cho phép mở cùng lúc nhiều phiên làm việc trên một máy tính.

Trình soạn thảo vi: Chương trình vi là một chương trình soạn thảo mạnh mà gần như chắc chắn được tìm thấy trên tất cả các hệ điều hành họ Linux, bởi kích thước và khả năng của vi không đòi hỏi nhiều tài nguyên, thêm vào đó là chức năng soạn thảo cơ bản, vi có thể tìm kiếm, thay thế, kết nối các file và nó có ngôn ngữ macro của chính nó, cũng như đặc điểm bổ sung. Có hai chế độ trong vi:

- chế độ thứ nhất là chế độ input: Trong chế độ này, văn bản được đưa vào trong tài liệu, bạn có thể chèn và bổ sung văn bản.
- chế độ thứ hai là chế độ dòng lệnh: Khi ở chế độ này, bạn có thể dịch chuyển trên tài liệu, trộn các dòng, tìm kiếm...Bạn có thể thực hiện tất cả các chức năng của vi từ chế độ dòng lệnh, ngoại trừ việc nhập văn bản

Tiện ích MC (Midnight Commander): Trong thời kỳ của DOS trước Windows, việc định hướng các tập tin thông qua hệ thống menu và các chương trình quản lý bắt đầu phát triển mạnh, cho dù chúng chỉ dựa trên chế độ text. Linux cũng có một chương trình tiện ích với chức năng tương tự như vậy gọi là Midnight Commander. Bạn không phải mất công tìm kiếm MC, phần lớn các nhà phân phối Linux đều cung cấp kèm theo HĐH và nó được cài trong /usr/bin/mc. Chương trình chạy ở hai chế độ textmode và đồ họa. MC có một số tính năng mà DOS không có. Bạn có thể thay đổi quyền sở hữu tập tin và xem chi tiết về quyền truy cập tập tin. MC còn có khả năng quản lý quy trình, cho phép bạn xem những quá trình đang được thực hiện ở chế độ nền, và bạn có thể dừng chúng, khởi động lại hoặc tắt chúng hoàn toàn

1.1.2.3. Giới thiệu hệ thống tập tin và thư mục

Các hệ thống máy tính sử dụng thiết bị lưu trữ ngoài để lưu trữ thông tin một cách bền vững. Các thiết bị lưu trữ quản lý không gian bộ nhớ ngoài theo từng khối dữ liệu. Giữa các khối dữ liệu chỉ liên quan về mặt vật lý, không có liên quan gì về mặt ngữ nghĩa. Để có thể sử dụng các khối dữ liệu này một cách thuận tiện, các khối dữ liệu có chung ngữ nghĩa, có chung mục đích sử dụng, được gộp lại với nhau và được quản lý bởi một khối dữ liệu điều khiển. Các khối dữ liệu gộp lại như vậy gọi là một tệp (file). Khi người

sử dụng có nhiều tệp, để có thể quản lý các tệp dễ dàng hơn, các tệp được gộp lại với nhau theo yêu cầu của người sử dụng, bổ sung thêm một tệp chứa danh mục và vị trí của các tệp được gộp. Tệp chứa danh mục này được gọi là tệp thư mục. Về phần mình, tệp thư mục cũng có thể được gộp vào với các tệp, khác để tạo thành thư mục. Với cách nhóm tệp như vậy, trong hệ thống sẽ có 2 loại tệp cơ bản:

- Tệp thông thường chỉ chứa dữ liệu.
- Tệp thư mục chỉ chứa danh mục các tệp và các thư mục con nằm trong thư mục đó.

Các tệp và các thư mục kết hợp với nhau tạo ra một hoặc nhiều cây thư mục, trong đó có các tệp thông thường là các nút lá. Nút gốc của các cây là các điểm cố định để từ đó có thể truy cập được nút lá trong cây. Ở dưới HĐH Linux, các tệp và thư mục tạo thành một cây duy nhất có thư mục gốc ký hiệu là / - (thư mục gốc). Các thư mục con thường gặp của thư mục gốc là các thư mục:

- /bin: thư mục tệp chương trình cơ bản
- /boot: thư mục chứa hạt nhân của HĐH
- /etc: thư mục chứa tệp cấu hình
- /dev: thư mục các tệp thiết bị
- /home: thư mục chứa dữ liệu người sử dụng
- /lib: thư viện hệ thống
- /usr: thư mục ứng dụng
- /var: thư mục dữ liệu cập nhật.
- /proc: thư mục chứa các dữ liệu của nhân hệ điều hành và BIOS

Các tệp thư mục lưu trữ các thư mục con và tệp. Các thư mục con và tệp đều được đặt tên. Giống như trong HĐH Windows, Linux cho phép tên tệp có thể dài đến 255 ký tự, có thể bao gồm các ký tự đặt biệt.

Để truy cập được vào các thư mục và tệp, xuất phát từ các nút gốc truy cập vào các thư mục con cho đến khi đến được tệp cần thiết. Tập hợp tên của các thư mục con từ nút gốc đến tệp cần truy cập, phân cách các tên bằng dấu /, gọi là đường dẫn tuyệt đối đến tệp. Trong mọi trường hợp, luôn luôn có thể dùng đường dẫn tuyệt đối để tham chiếu tới tệp.

Khi người sử dụng truy cập vào hệ thống hoặc khi các chương trình đang thực hiện, một thư mục được sử dụng để tham chiếu tới tất cả các tệp và thư mục khác trong hệ thống. Với người sử dụng đó thường là thư mục /home. Với chương trình, đó thường là thư mục gọi câu lệnh thực hiện, thư mục này được gọi là thư mục làm việc hiện tại.

Trong một thư mục luôn luôn có 2 thư mục đặc biệt: ./ để biểu diễn thư mục hiện tại và ../ biểu diễn thư mục cha của thư mục hiện tại.

Trong nhiều trường hợp, sẽ hiệu quả hơn nếu truy cập vào một tệp thông qua đường đi trong cây từ thư mục hiện tại đến tệp cần truy cập bằng cách sử dụng ./ và ../. Một đường dẫn như vậy sẽ phụ thuộc vào thư mục làm việc hiện tại, được gọi là đường dẫn tương đối.

1.1.3. Phân loại phần mềm nguồn mở

1.1.3.1. Theo phương thức hoạt động

Phần mềm hệ thống: dùng để vận hành máy tính và các phần cứng máy tính, ví dụ như các hệ điều hành máy tính Windows XP, Linux, Unix, các thư viện động DLL (Dynamic Link Library) của hệ điều hành, các trình điều khiển (driver), phần sụn firmware và BIOS.

Phần mềm ứng dụng: để người dùng có thể hoàn thành một hay nhiều công việc nào đó, ví dụ như phần mềm văn phòng, phần mềm doanh nghiệp, phần mềm quản lý nguồn nhân lực

Phần mềm chuyển dịch mã bao gồm trình biên dịch và thông dịch: các loại chương trình này sẽ đọc các câu lệnh từ các mã nguồn được viết bởi lập trình viên bằng một ngôn ngữ lập trình và dịch nó sang ngôn ngữ máy mà máy tính có thể hiểu được.

1.1.3.2. Theo khả năng ứng dụng

Những phần mềm không phụ thuộc, nó có thể được bán cho bất kỳ khách hàng nào trên thị trường tự do. Ví dụ phần mềm về cơ sở dữ liệu Oracle, Photoshop... Những phần mềm được viết theo đơn đặt hàng hay hợp đồng của một khách hàng cụ thể nào đó (một công ty, bệnh viện, trường học...)

1.1.3.3. Theo điều kiện sử dụng

Phần mềm mã nguồn mở, FreeWare, ShareWare

1.1.3.4. Theo hiệu quả xã hội

Phần mềm độc hại, Phần mềm giáo dục

1.1.3.5. Theo kích thước

Phần mềm khổng lồ, phần mềm mini

1.1.4. Phân biệt phần mềm nguồn mở với một số phần mềm khác

1.1.4.1. Phần mềm sở hữu

Là phần mềm có bản quyền ràng buộc chặt chẽ các thao tác trên phần mềm, đảm bảo quyền lợi của người làm ra phần mềm. Copy Right (bản quyền) là thuật ngữ chỉ quyền quản lý đối với phần mềm, cho phép / không cho phép thực hiện các thao tác trên phần mềm. Với các phần mềm sở hữu, thông thường bản quyền có các ràng buộc chặt chẽ đảm bảo quyền lợi của người làm ra phần mềm. Do đó, bản quyền của các phần mềm chủ sở hữu thường rất chặt chẽ về quyền phân phối và quản lý, hạn chế quyền thay đổi và cải tiến và hầu như không cho phép việc phân tích ngược mã. Ví dụ: MS Office, Photoshop...

1.1.4.2. Phần mềm miễn phí

Là phần mềm không mất phí sử dụng nhưng không nhất thiết là mã nguồn mở. Phần mềm sẽ được phân phối kèm theo tất cả các quyền, trừ quyền quản lý. Các chủ thể có thể sử dụng hoàn toàn tự do phần mềm, trừ việc sử dụng quyền quản lý để áp đặt hạn chế lên các quyền còn lại. Các phần mềm được phân phối theo cách thức này được gọi là phần mềm tự do hay phần mềm miễn phí. Ví dụ: Yahoo Messenger, Skype, IE,...

1.1.4.3. Phần mềm chia sẻ

Phần mềm cung cấp miễn phí với một số hạn chế chức năng hoặc mức độ thuận tiện. Người dùng chỉ có đầy đủ chức năng khi trả tiền mua giấy phép.

CHƯƠNG 2 : CÔNG NGHỆ VPN VÀ CÁC GIAO THỨC HỖ TRỢ

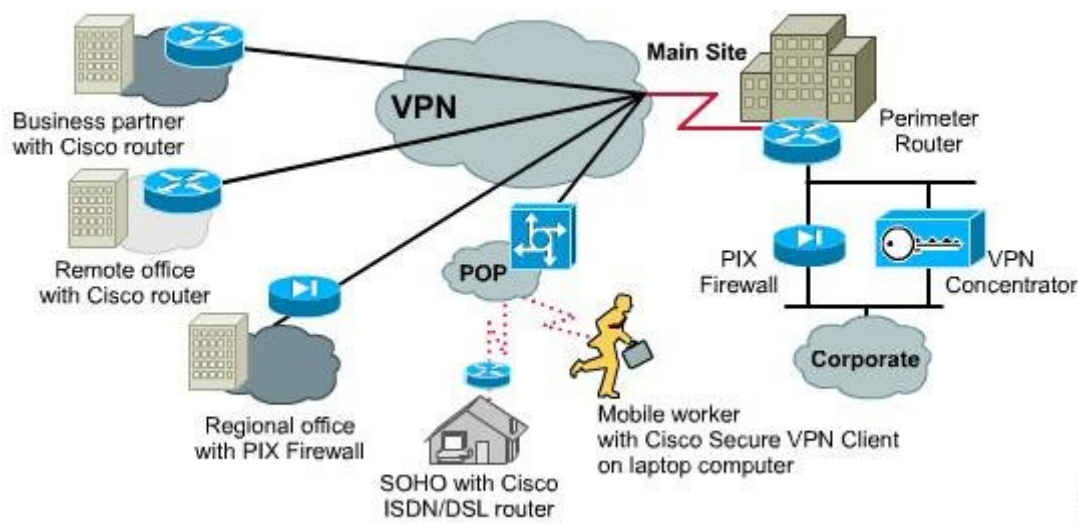
2.1. TỔNG QUAN VỀ CÔNG NGHỆ VPN

2.1.1. Giới thiệu về công nghệ VPN

VPN là một mô hình mạng mới tận dụng lại những cơ sở hạ tầng hiện có của Internet. Với mô hình mạng mới này, người ta không phải đầu tư thêm nhiều về cơ sở hạ tầng mà các tính năng như bảo mật, độ tin cậy đảm bảo, đồng thời có thể quản lý riêng được sự hoạt động của mạng này. VPN cho phép người sử dụng làm việc tại nhà, trên đường đi hay văn phòng chi nhánh có kết nối an toàn đến máy chủ. Trong nhiều trường hợp VPN cũng giống như WAN (Wire Area Network), tuy nhiên đặt tính quyết định của VPN là chúng có thể dùng mạng công cộng như Internet mà đảm bảo tính riêng tư và tiết kiệm hơn nhiều.

2.1.2. Định nghĩa VPN

VPN được hiểu đơn giản như là sự mở rộng của một mạng riêng (private network) thông qua các mạng công cộng. Về căn bản, mỗi VPN là một mạng riêng lẻ sử dụng một mạng chung (thường là internet) để kết nối cùng các site (các mạng riêng lẻ) hay nhiều người dùng từ xa. Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường lease line, mỗi VPN sử dụng các kết nối ảo được dẫn đường qua Internet từ mạng riêng của công ty tới các site hay các nhân viên từ xa. Để có thể gửi và nhận dữ liệu thông qua mạng công cộng mà vẫn đảm bảo tính an toàn và bảo mật, VPN cung cấp cơ chế mã hóa dữ liệu trên đường truyền tạo ra một đường ống bảo mật giữa nơi nhận và nơi gửi (Tunnel) giống như một kết nối point-to-point trên mạng riêng. Để có thể tạo ra một đường ống bảo mật đó, dữ liệu phải được mã hóa hay che dấu đi, chỉ cung cấp phần đầu gói dữ liệu (header) là thông tin về đường đi cho phép nó có thể đi đến đích thông qua mạng công cộng một cách nhanh chóng. Dữ liệu được mã hóa một cách cẩn thận do đó nếu các packet bị bắt lại trên đường truyền công cộng cũng không thể đọc được nội dung vì không có khóa để giải mã. Liên kết với dữ liệu được mã hóa và đóng gói được gọi là kết nối VPN. Các đường kết nối VPN thường được gọi là đường ống VPN (VPN Tunnel).



Hình 2.1. Minh họa mô hình kết nối VPN

VPNs có thể sử dụng một hoặc cả hai kỹ thuật: dùng các kênh thuê bao riêng của các nhà cung cấp dịch vụ (cái này gọi là một *Trusted VPN*) hoặc gửi các dữ liệu đã được mã hóa lên mạng Internet (cái này gọi là *Secure VPN*). Dùng một *Secure VPN* qua một *Trusted VPN* thì gọi là *Hybrid VPN*. Kết hợp cả hai loại của *Secure VPN* trong một cổng vào, chẳng hạn như IPsec và SSL cũng gọi là *Hybrid VPN*.

Qua nhiều năm, các *Trusted VPN* đã có sự thay đổi từ các thuê bao riêng từ các đại lý viễn thông đến các thuê bao IP riêng từ các nhà cung cấp dịch vụ Internet. Công nghệ chủ yếu của sự vận hành của *Trusted VPN* với mạng địa chỉ IP là các kênh ATM, mạch tiếp sóng khung, và MPLS.

ATM và bộ tiếp sóng khung hoạt động tại tầng liên kết dữ liệu, là tầng 2 trong mô hình OSI (tầng 1 là tầng vật lý, tầng 3 là tầng mạng). MPLS mô phỏng một số thuộc tính của mạng chuyển mạch và mạng chuyển gói. Nó hoạt động cùng một tầng, thường được coi là tầng “2,5” vì nó nằm ngay giữa tầng liên kết và tầng mạng. MPLS bắt đầu thay thế ATM và bộ tiếp sóng khung để thực thi *Trusted VPN* với lượng lớn các doanh nghiệp và nhà cung cấp dịch vụ.

Secure VPN có thể dùng IPsec trong việc mã hóa. IPsec nằm trong giao thức L2TP (*Layer 2 Tunneling Protocol*), trong thành phần SSL (*Secure Sockets Layer*) 3.0 hay trong

TLS (*Transport Layer Security*) với bộ mã hoá, L2F (*Layer Two Forwarding*) hay PPTP (*Point-to-Point Tunneling Protocol*). Chúng ta hãy xem qua các thành phần chính này.

IPsec hay IP security – là tiêu chuẩn cho sự mã hoá cũng như cho thẩm định các gói IP tại tầng mạng. IPsec có một tập hợp các giao thức mật mã với 2 mục đích: an ninh gói mạng và thay đổi các khoá mật mã. Một số chuyên gia an ninh như Bruce Schneier của Counterpane Internet Security, đã xem IPsec như là một giao thức cho VPNs từ cuối những năm 1990. IPsec được hỗ trợ trong Windows XP, 2000, 2003 và Vista; trong Linux 2.6 và các phiên bản sau; trong Mac OS X, Net BDS, FreeBSD và OpenBDS, trong Solari, AIX, và HP-UX, trong VxWorks. Nhiều đã cung cấp dịch vụ IPsec VPN server và IPsec VPN client.

L2TP/IPsec kết hợp đường dẫn ảo của L2TP với kênh an toàn của IPsec. Nó cho phép thay đổi Internet Key Exchange dễ dàng hơn so với thuần IPsec. Microsoft đã cung cấp một bản VPN client L2TP/IPsec miễn phí cho Windows 98, ME, và NT từ năm 2002, và gắn một VPN client L2TP/IPsec cho Windows XP, 2000, 2003 và Vista. Windows server 2003 và Windows 2000 server có L2TP/IPsec server.

SSL và TLS là các giao thức cho luồng dữ liệu an toàn tại tầng 4 của mô hình OSI. SSL 3.0 và TLS 1.0 là các bản thừa kế được dùng phổ biến với HTTP nhằm cho phép bảo vệ các đường dẫn Web an toàn, gọi là HTTPS. Tuy nhiên SSL/TLS cũng được dùng để tạo ra một đường dẫn ảo tunnel VPN. Ví dụ: OpenVPN là một gói VPN nguồn mở cho Linux, xBSD, Mac OS X, Pocket PCs và Windows 2000, XP, 2003, và Vista. Nó dùng SSL để cung cấp mã hoá cho cả dữ liệu và kênh điều khiển. Một vài hãng đã cung cấp SSL VPN server và client.

2.1.3. Lợi ích của VPN

Một mạng riêng ảo có thể xóa bỏ các hàng rào địa lý trong kinh doanh, cho phép các nhân viên làm việc một cách hiệu quả tại nhà và cho phép một doanh nghiệp kết nối một cách an toàn tới các đại lý của họ cùng các hãng hợp tác. Một mạng riêng ảo thường rẻ hơn và có hiệu quả hơn các đường riêng ảo.

Nhưng mặt khác, cách dùng của một VPN có thể phô bày các rủi ro an ninh tiềm ẩn. Trong khi hầu hết các mạng riêng ảo đang được dùng khá an toàn thì một mạng riêng

ảo cũng có thể làm cho chính nó khó phá hoại hơn bằng cách bảo vệ tham số của mạng một cách thích hợp. Phận sự của người quản trị mạng là áp dụng các tiêu chuẩn an ninh giống nhau trong việc kết nối các máy tính tới mạng thông qua VPN khi các máy tính kết nối trực tiếp vào mạng LAN.

Kết hợp đồng thời cách dùng của cả hai kiểu VPNs có thể thấy được tiềm năng mạng của công ty này với công ty khác. Thêm vào đó, sử dụng phần mềm điều khiển từ xa như PC Anywhere, GoToMyPC hay VNC kết hợp với một VPN có thể khai thác được khả năng mạng của công ty tới các malware trong một máy trạm xa không kết nối VPN.

Bởi Secure VPN sử dụng mã hoá, và vì một số hàm mật mã được dùng khá là đắt tiền nên một VPN được dùng khá nặng có thể tải xuống server của nó. Đặc thù của người quản trị là quản lí việc tải server bằng cách giới hạn số kết nối đồng thời để biết server nào có thể điều khiển.

Khi số người cố gắng kết nối tới VPN đột nhiên tăng vọt đến đỉnh điểm, phá vỡ hết quá trình truyền tin, các nhân viên cũng thấy chính họ không thể kết nối được. Vì tất cả các cổng của VPN đều bận. Điều đó chính là động cơ thúc đẩy người quản trị tạo ra các khoá ứng dụng làm việc mà không đòi hỏi VPN. Chẳng hạn thiết lập dịch vụ proxy hoặc dịch vụ Internet Message Access Protocol để cho phép nhân viên truy cập e-mail từ nhà hay trên đường.

VPN cung cấp nhiều đặc tính hơn so với những mạng truyền thống và những mạng lease-line. Những lợi ích đầu tiên bao gồm:

- Chi phí thấp hơn những mạng riêng: VPN có thể giảm chi phí khi truyền tới 20-40% so với những mạng thuộc mạng lease-line và giảm việc chi phí truy cập từ xa từ 60-80%.
- Tính linh hoạt cho khả năng kinh tế trên Internet. VPN vốn đã có tính linh hoạt và có thể leo thang những kiến trúc mạng hơn là mạng cổ điển, bằng cách đó nó có thể hoạt động kinh doanh nhanh chóng và chi phí một cách hiệu quả cho việc kết nối mở rộng. Theo cách này VPN có thể dễ dàng kết nối hoặc ngắt kết nối từ xa của những văn phòng, những vị trí ngoài quốc tế, những người truyền thông, những người dùng điện

thoại di động, những người hoạt động kinh doanh bên ngoài như những yêu cầu kinh doanh đã đòi hỏi.

- Đơn giản hóa những gánh nặng.
- Những cấu trúc mạng ồng, vì thế giảm việc quản lý những gánh nặng. Sử dụng một giao thức Internet backbone loại trừ những PVC tích hợp với kết nối hướng những giao thức như là Frame Relay và ATM
- Tăng tính bảo mật: các dữ liệu quan trọng sẽ được che giấu đối với những người không có quyền truy cập và cho phép truy cập đối với những người dùng có quyền truy cập.
- Hỗ trợ các giao thức mạng thông dụng hiện nay như TCP/IP.
- Bảo mật địa chỉ IP: bởi vì thông tin được gửi đi trên VPN đã được mã hóa do đó các địa chỉ bên trong mạng riêng được che giấu và chỉ sử dụng các địa chỉ bên ngoài Internet.

2.1.4. Các thành phần cần thiết để tạo kết nối VPN

- *User Authentication*: cung cấp cơ chế chứng thực người dùng, chỉ cho phép người dùng hợp lệ kết nối và truy cập hệ thống VPN.
- *Address Management*: cung cấp địa chỉ IP hợp lệ cho người dùng sau khi gia nhập hệ thống VPN để có thể truy cập tài nguyên mạng nội bộ.
- *Data Encryption*: cung cấp giải pháp mã hóa dữ liệu trong quá trình truyền nhằm đảm bảo tính riêng tư và toàn vẹn dữ liệu.
- *Key Management*: cung cấp giải pháp quản lý các khóa dùng cho quá trình mã hóa và giải mã dữ liệu.

2.2. CÁC GIAO THỨC VPN

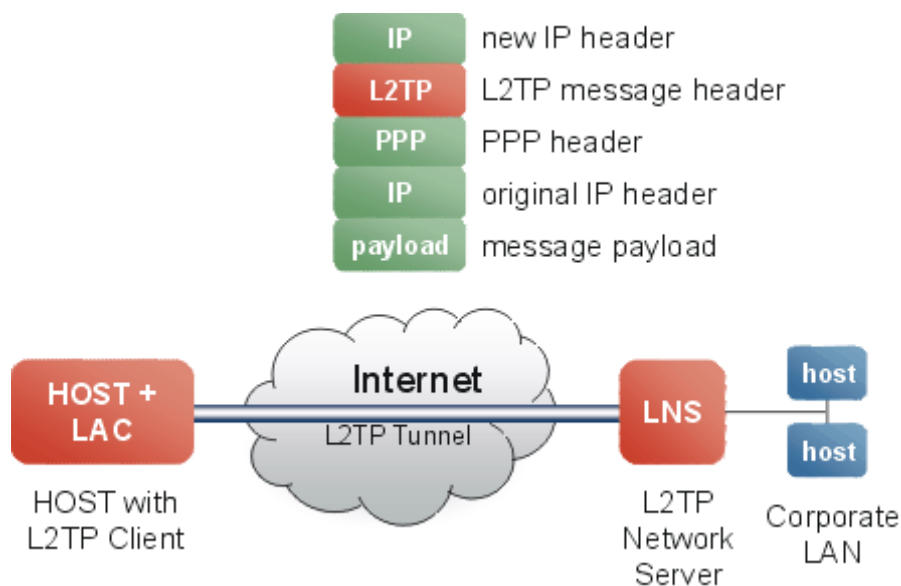
2.2.1. L2TP

Trước khi xuất hiện chuẩn L2TP (tháng 8 năm 1999), Cisco sử dụng Layer 2 Forwarding (L2F) như là giao thức chuẩn để tạo kết nối VPN. L2TP ra đời sau với những tính năng được tích hợp từ L2F.

L2TP là dạng kết hợp của Cisco L2F và Microsoft Point-to-Point Tunneling Protocol (PPTP). Microsoft hỗ trợ chuẩn PPTP và L2TP trong các phiên bản WindowNT và 2000

L2TP được sử dụng để tạo kết nối độc lập, đa giao thức cho mạng riêng ảo quay số (Virtual Private Dial-up Network). L2TP cho phép người dùng có thể kết nối thông qua các chính sách bảo mật của công ty (security policies) để tạo VPN hay VPDN như là sự mở rộng của mạng nội bộ công ty.

L2TP không cung cấp mã hóa



Hình 2.2. Giao thức L2TP

L2TP là sự kết hợp của PPP (giao thức Point-to-Point) với giao thức L2F (Layer 2 Forwarding) của Cisco do đó rất hiệu quả trong kết nối mạng dial, ADSL và các mạng truy cập từ xa khác. Giao thức mở rộng này sử dụng PPP để cho phép truy cập VPN bởi những người sử dụng từ xa.

2.2.2. GRE

Đây là đa giao thức truyền thông đóng gói IP, CLNP và tất cả các gói dữ liệu bên trong đường ống IP (IP Tunnel).

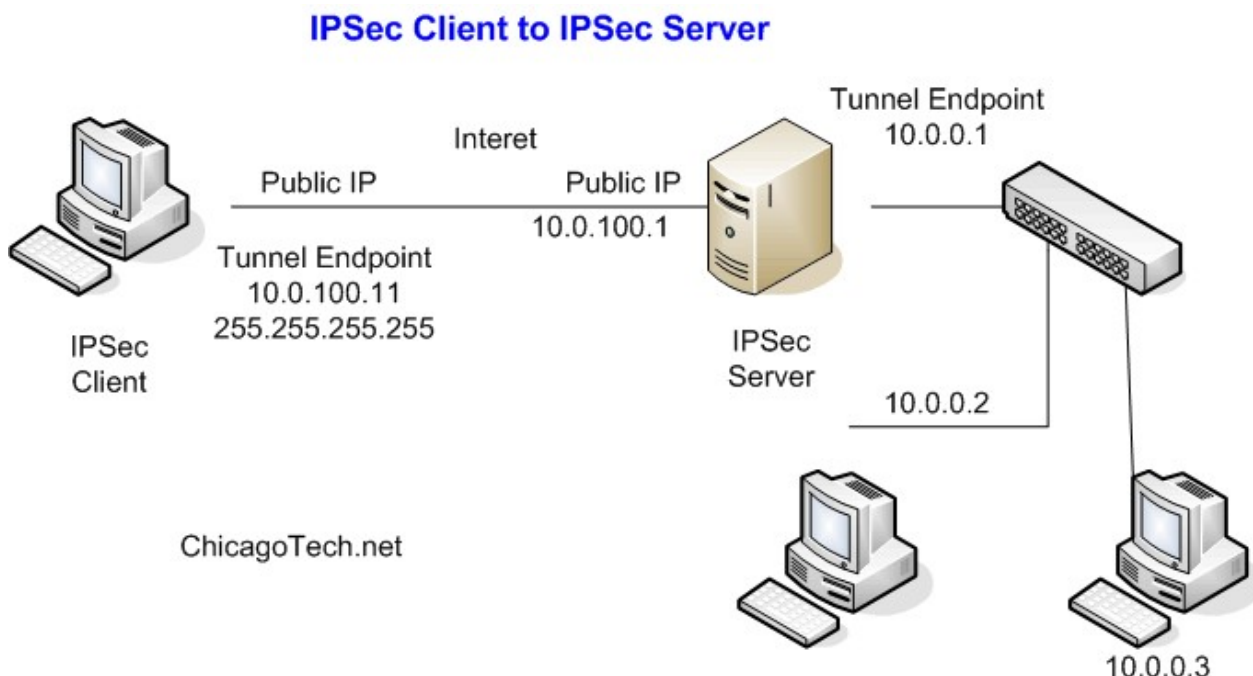
Với GRE Tunnel, Cisco router sẽ đóng gói cho mỗi vị trí một giao thức đặc trưng chỉ định trong gói IP header, tạo một đường kết nối ảo (virtual point-to-point) tới Cisco router cần đến. Và khi gói dữ liệu đến đích IP header sẽ được mở ra.

Bằng việc kết nối nhiều mạng con với giao thức khác nhau trong môi trường có một giao thức chính. GRE Tunneling cho phép các giao thức khác có thể thuận lợi trong việc định tuyến cho gói IP

2.2.3. IPSec

IPSec là sự lựa chọn cho việc bảo mật trên VPN. IPSec là một khung bao gồm bảo mật dữ liệu (data confidentiality), tính toàn vẹn của dữ liệu và việc chứng thực dữ liệu.

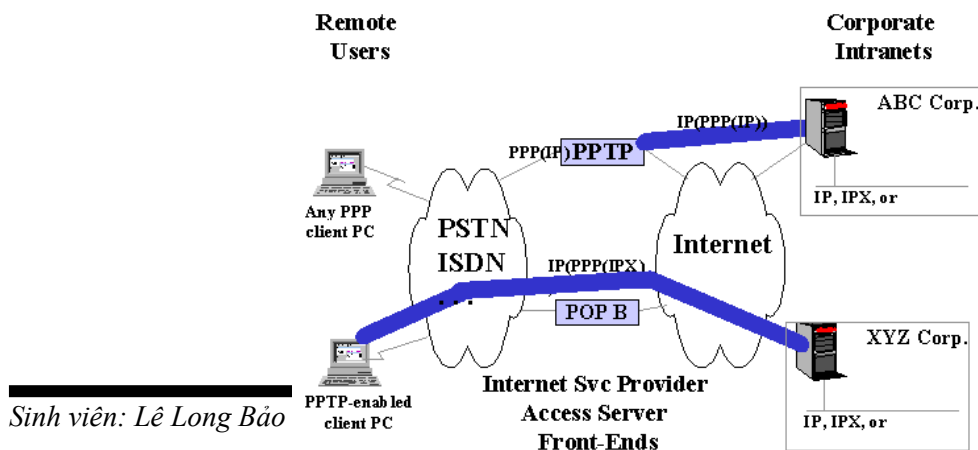
IPSec cung cấp dịch vụ bảo mật ứng dụng KDE cho phép thỏa thuận các giao thức và thuật toán trên nền chính sách cục bộ (group policy) và sinh ra các khóa bảo mật mã hóa và chứng thực được sử dụng trong IPSec



Hình 2.3. IPSec

2.2.4. PPTP (Point to Point Tunneling Protocol)

Được sử dụng trên các máy client chạy hệ điều hành Microsoft for NT4.0 và Windows 95+. Giao thức này được sử dụng để mã hóa dữ liệu lưu thông trên mạng LAN. Giống như giao thức NETBEUI và IPX trong một packet gửi lên Internet. PPTP dựa trên chuẩn RSA RC4 và hỗ trợ bởi sự mã hóa 40-bit hoặc 128-bit



Hình 2.4. Giao thức PPTP

2.3. KẾT NỐI VPN

2.3.1. Các dạng kết nối VPN

2.3.1.1. Remote Access VPNs

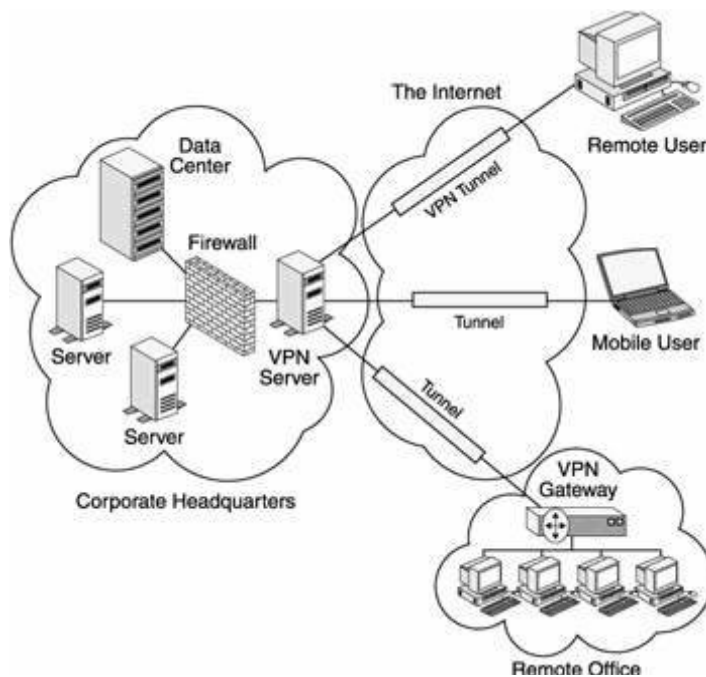
Remote Access VPNs cho phép truy cập bất cứ lúc nào bằng Remote, mobile và các thiết bị truyền thông của nhân viên các chi nhánh kết nối đến tài nguyên mạng của tổ chức.

Remote Access VPNs mô tả việc các người dùng ở xa sử dụng các phần mềm VPN để truy cập vào mạng Intranet của công ty thông qua gateway hoặc VPN concentrator (bản chất là một server). Vì lý do này, giải pháp này thường được gọi là client/server. Trong giải pháp này, các người dùng thường sử dụng các công nghệ WAN truyền thống để tạo lại các tunnel về mạng HO (Home Office) của họ.

Một hướng phát triển khá mới trong remote access VPN là dùng wireless VPN, trong đó một nhân viên có thể truy cập về mạng của họ thông qua kết nối không dây. Trong thiết kế này, các kết nối không dây cần phải kết nối về một trạm wireless (wireless terminal) và sau đó về mạng của công ty. Trong cả hai trường hợp, phần mềm client trên máy PC đều cho phép khởi tạo các kết nối bảo mật, còn được gọi là tunnel.

Một phần quan trọng của thiết kế này là việc thiết kế quá trình xác thực ban đầu nhằm để đảm bảo là yêu cầu được xuất phát từ một nguồn tin cậy. Thường thì giai đoạn ban đầu này dựa trên cùng một chính sách về bảo mật của công ty. Chính sách bao gồm: qui trình (procedure), kỹ thuật, server, Terminal Access Controller,...

Bằng việc triển khai Remote Access VPNs, những người dùng từ xa hoặc các chi nhánh văn phòng chỉ cần cài đặt một kết nối cục bộ đến nhà cung cấp dịch vụ ISP hoặc ISP's POP và kết nối đến tài nguyên thông qua Internet.



Hình 2.5. Remote Access VPN

Như hình trên bạn có thể suy ra, thuận lợi chính của Remote Access VPNs:

- Sự cần thiết của RAS và việc kết hợp với modem được loại trừ.
- Sự cần thiết hỗ trợ cho người dùng cá nhân được loại trừ bởi vì kết nối từ xa đã được tạo điều kiện thuận lợi bởi ISP
- Việc quay số từ những khoảng cách xa được loại trừ, thay vào đó, những kết nối với khoảng cách xa sẽ được thay thế bởi các kết nối cục bộ.
- Giảm giá thành chi phí cho các kết nối với khoảng cách xa
- Do đây là một kết nối mang tính cục bộ, do vậy tốc độ kết nối sẽ cao hơn so với kết nối trực tiếp đến những khoảng cách xa
- VPNs cung cấp khả năng truy cập đến trung tâm tốt hơn bởi vì nó hỗ trợ dịch vụ truy cập ở mức độ tối thiểu nhất cho dù có sự tăng nhanh chóng các kết nối đồng thời đến mạng

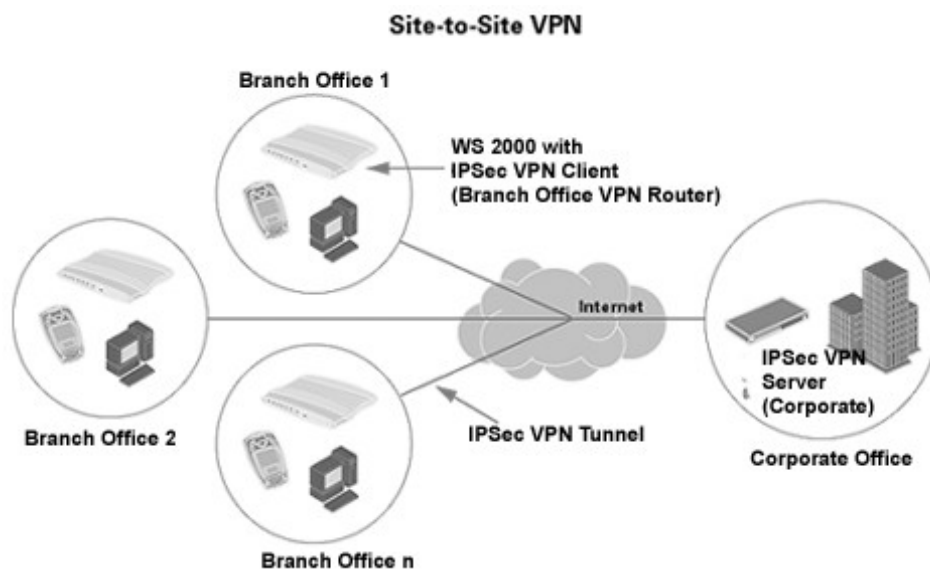
Ngoài những thuận lợi trên, thì VPN cũng có những điểm bất lợi như:

- Remote Access VPNs cũng không bảo đảm được chất lượng phục vụ

- Khả năng mất dữ liệu là rất cao, thêm nữa là các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất thoát
- Do độ phức tạp của thuật toán mã hóa, protocol overhead tăng đáng kể, điều này gây khó khăn cho quá trình xác nhận. Thêm vào đó việc nén dữ liệu IP và PPP-based diễn ra vô cùng chậm chạp và tồi tệ
- Do phải truyền dữ liệu thông qua Internet, nên khi trao đổi các dữ liệu lớn như các gói dữ liệu truyền thông, phim ảnh, âm thanh sẽ rất chậm.

2.3.1.2. Site-to-Site (Lan-to-Lan)

Site-to-site VPN được áp dụng để cài đặt mạng từ một vị trí này kết nối tới mạng của một vị trí khác thông qua VPN. Trong hoàn cảnh này thì việc chứng thực ban đầu giữa các thiết bị mạng được giao cho người sử dụng. Nơi mà có một kết nối VPN được thiết lập giữa chúng. Khi đó các thiết bị này đóng vai trò như là một gateway, và đảm bảo rằng việc lưu thông đã được dự tính trước cho các site khác. Các router và Firewall tương thích với VPN, và các bộ tập trung VPN chuyên dụng đều cung cấp chức năng này.



Hình 2.6. Site to Site VPN

Lan-to-Lan có thể được xem như là intranet VPN hoặc extranet VPN. Nếu chúng ta xem xét dưới góc độ chứng thực nó có thể được xem như là một intranet VPN, ngược

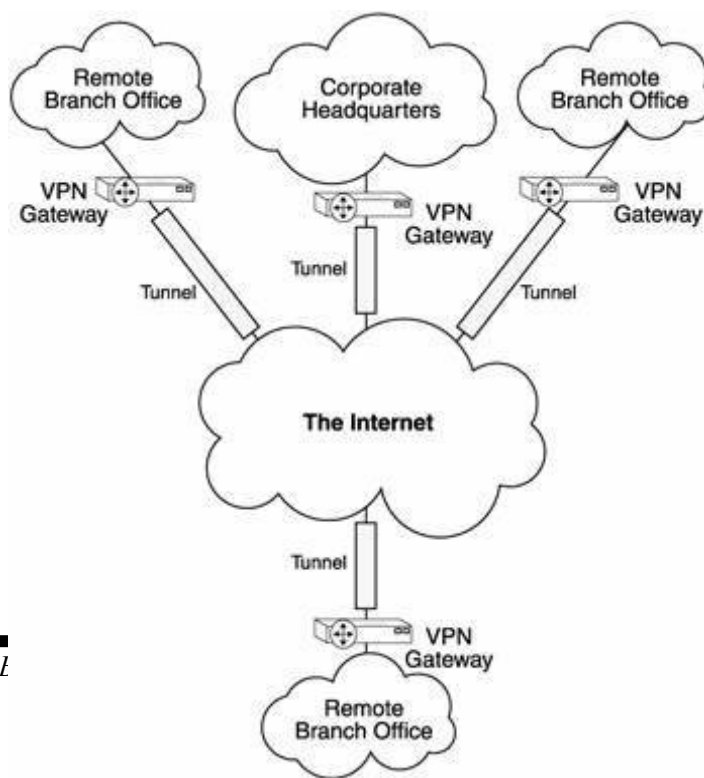
lại chúng được xem như là một extranet VPN. Tính chất chễ trong việc truy cập giữa các site có thể được điều khiển bởi cả hai (intranet và extranet VPN) theo các site tương ứng của chúng. Giải pháp Site to Site VPN không phải là một remote access VPN nhưng nó được thêm vào đây là vì tính chất hoàn thiện của nó

Sự phân biệt giữa remote access VPN và Lan to Lan chỉ đơn thuần mang tính chất tượng trưng và xa hơn là nó được cung cấp cho mục đích thảo luận. Ví dụ như là các thiết bị VPN dựa trên phần cứng mới, ở đây để phân loại được, chúng ta phải áp dụng cả hai cách, bởi vì hardware-based client có thể xuất hiện nếu một thiết bị đang truy cập vào mạng. Mặc dù một mạng có thể có nhiều thiết bị VPN đang vận hành.

Lan to Lan VPN là sự kết nối hai mạng riêng lẻ thông qua một đường hầm bảo mật, đường hầm bảo mật này có thể sử dụng các giao thức PPTP, L2TP, hoặc IPSec, mục đích của Lan to Lan là kết nối hai mạng không có đường nối lại với nhau, không có việc thỏa hiệp tích hợp, chứng thực, sự cản mật của dữ liệu, bạn có thể thiết lập một Lan to Lan VPN thông qua sự kết hợp của các thiết bị VPN Concentrators, Routers, và Firewalls.

Kết nối Lan to Lan được thiết kế để tạo một kết nối mạng trực tiếp, hiệu quả bất chấp khoảng cách vật lý giữa chúng. Có thể kết nối này luân chuyển thông qua internet hoặc một mạng không được tin cậy. Bạn phải đảm bảo vấn đề bảo mật bằng cách sử dụng sự mã hóa dữ liệu trên tất cả các gói dữ liệu đang luân chuyển giữa các mạng đó.

Intranet VPNs: được sử dụng để kết nối đến các chi nhánh văn phòng của tổ chức đến Backbone Router sử dụng campus router. Theo như mô hình bên dưới sẽ rất tốn chi phí do phải sử dụng 2 router để thiết lập mạng, triển khai, bảo Intranet kém còn tùy lưu thông.

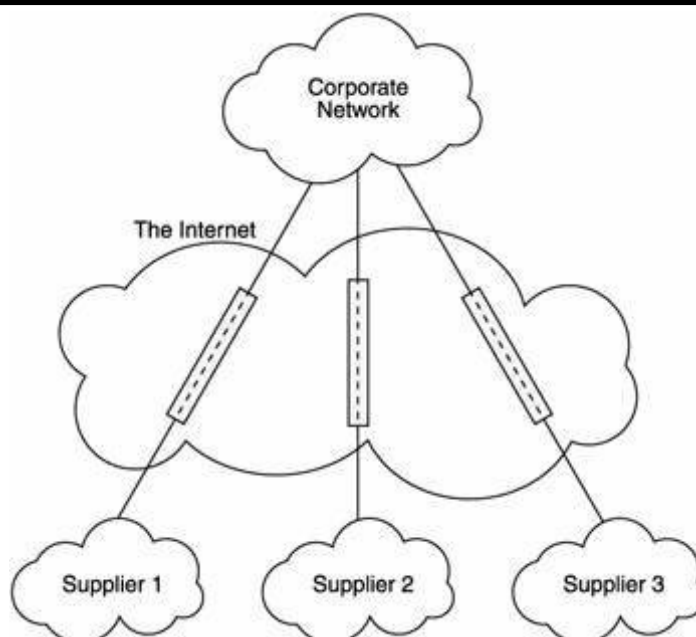


Hình 2.7. Intranet VPNs

Để giải quyết vấn đề trên, sự tồn kém của WAN backbone được thay thế bởi các kết nối Internet với chi phí thấp. Với mô hình như vậy hiệu quả chi phí hơn, do giảm số lượng router được sử dụng theo mô hình WAN backbone. Giảm thiểu đáng kể số lượng hỗ trợ yêu cầu người dùng cá nhân qua toàn cầu, các trạm ở một số remote site khác nhau. Kết nối nhanh hơn, tốt hơn.

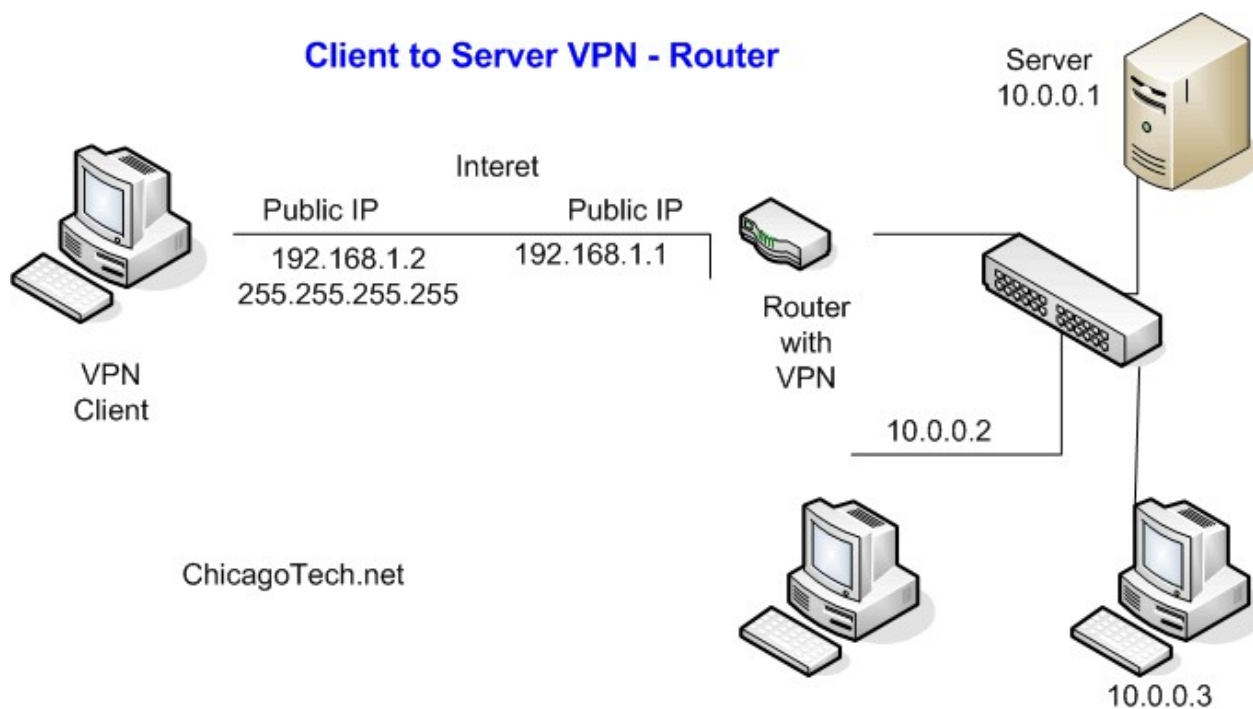
Extranet VPNs: Không giống như Intranet và Remote Access-based, Extranet không hoàn toàn cách li từ bên ngoài, Extranet cho phép truy cập những tài nguyên mạng cần thiết của các đối tác kinh doanh, chẳng hạn như khách hàng, nhà cung cấp, đối tác những người giữ vai trò quan trọng trong tổ chức.

Do hoạt động trên môi trường Internet, bạn có thể lựa chọn nhà phân phối khi lựa chọn và đưa ra phương pháp giải quyết tùy theo nhu cầu của tổ chức. Bởi vì một phần Internet – Connectivity được bảo trì bởi nhà cung cấp ISP nên cũng giảm chi phí bảo trì khi thuê nhân viên bảo trì. Dễ dàng triển khai, quản lý và chỉnh sửa thông tin.



Hình 2.8. Extranet VPNs

2.3.2. Thiết lập một kết nối VPN



Hình 2.9. Thiết lập một kết nối Client to Server

Máy VPN cần kết nối (VPN Client) tạo kết nối VPN tới máy chủ cung cấp dịch vụ VPN (VPN Server) thông qua kết nối Internet.

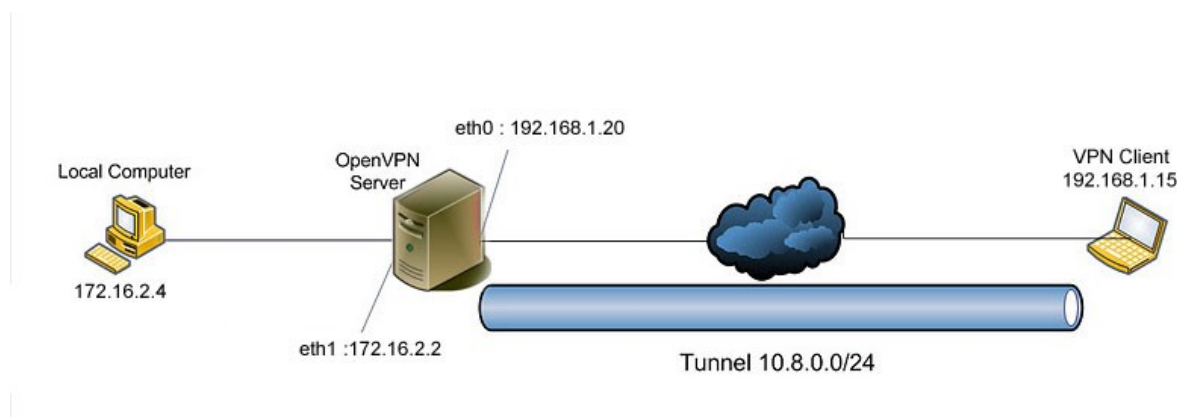
Máy chủ cung cấp dịch vụ VPN trả lời kết nối tới

Máy chủ cung cấp dịch vụ VPN chứng thực cho kết nối và cấp phép cho kết nối

Bắt đầu trao đổi dữ liệu giữa máy cần kết nối VPN và mạng công ty

CHƯƠNG 3: MÔ HÌNH HỆ THỐNG VÀ TRIỂN KHAI OPENVPN TRÊN UBUNTU SERVER

3.1. MÔ HÌNH HỆ THỐNG



Hình 3.1. Mô hình hệ thống

Mô hình hệ thống gồm 1 máy OpenVPN Server Linux, hệ điều hành Ubuntu Server, một máy VPN Client, một máy Local Computer nằm trong miền mạng của doanh nghiệp.

VPN Client: 192.168.1.15

OpenVPN Server: 172.16.2.2 - 192.168.1.20

Local Computer: 172.16.2.4

VPN Client sẽ quay kết nối tới máy OpenVPN Server và trao đổi dữ liệu với máy Local Computer nằm trong miền mạng LAN của doanh nghiệp.

Quá trình quay kết nối sẽ tạo ra một đường hầm với các IP nguồn và đích được mã hóa ẩn dấu, và thay vào đó là IP của OpenVPN : 10.8.0.0/24 với giao thức mã hóa là PPTP, và các IP này sẽ được gán cho Server và VPNClient

3.2. CÀI ĐẶT VÀ CẤU HÌNH OPENVPN

3.2.1. Cài đặt OpenVPN trên Ubuntu Server

```
longbaoitc@ubuntu:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:90:71:48
          inet addr:192.168.1.20  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe90:7148/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:512 (512.0 B)  TX bytes:2926 (2.9 KB)
          Interrupt:19 Base address:0x2000

longbaoitc@ubuntu:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:90:71:52
          inet addr:172.16.2.2  Bcast:172.16.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe90:7152/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:256 (256.0 B)  TX bytes:706 (706.0 B)
          Interrupt:19 Base address:0x2080

longbaoitc@ubuntu:~$ _
```

Hình 3.2. Kiểm tra cấu hình IP

```
longbaoitc@ubuntu:~$ sudo apt-get install openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libpkcs11-helper1 openssl-blacklist openvpn-blacklist
Suggested packages:
  resolvconf
The following NEW packages will be installed:
  libpkcs11-helper1 openssl-blacklist openvpn openvpn-blacklist
0 upgraded, 4 newly installed, 0 to remove and 89 not upgraded.
Need to get 0B/7,875kB of archives.
After this operation, 16.1MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Preconfiguring packages ...
Selecting previously deselected package openssl-blacklist.
(Reading database ... 80%_
```

Hình 3.3. Cài đặt OpenVPN trên Ubuntu Server

➤ Để cài đặt phần mềm chúng ta dùng lệnh :

Sudo apt-get install openvpn

3.2.2. Cấu hình các chức năng OpenVPN trên Ubuntu Server

```
root@ubuntu:/home/longbaoitc# cp -r /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn
root@ubuntu:/home/longbaoitc# _
```

Hình 3.4. Copy file cấu hình mẫu vào thư mục openvpn

➤ Tiến hành copy các file cấu hình mẫu từ thư mục /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz và thư mục /etc/openvpn.



```
GNU nano 2.2.4 File: vars
export CA_EXPIRE=3650
# In how many days should certificates expire?
export KEY_EXPIRE=3650
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="VIETNAM"
export KEY_PROVINCE="TP DANANG"
export KEY_CITY="DN"
export KEY_ORG="VIETHAN"
export KEY_EMAIL="lelongbao2790@gmail.com"
```

Hình 3.5. Chỉnh thông tin trong file vars

➤ Chỉnh các thông tin trong file vars như sau:

KEY_COUNTRY: Nhập tên nước

KEY_CITY: Nhập tên thành phố

KEY_ORG: Nhập tên tổ chức

KEY_EMAIL: Nhập email của người quản trị

➤ Sau đó thoát và lưu các thông tin cấu hình trong file vars và load lại bằng lệnh:

source ./vars

➤ Tiến hành xây dựng chứng thực CA key

```
root@ubuntu:/etc/openvpn/easy-rsa/2.0# ./clean-all
root@ubuntu:/etc/openvpn/easy-rsa/2.0# ./build-ca
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VIETNAM]:
string is too long, it needs to be less than 2 bytes long
Country Name (2 letter code) [VIETNAM]:VN
State or Province Name (full name) [TP DANANG]:
Locality Name (eg, city) [DN]:
Organization Name (eg, company) [VIETHAN]:
Organizational Unit Name (eg, section) []:MM03A_
```

Hình 3.6. Build CA

➤ Tạo các user để các VPNClient đăng nhập sau này

```
root@ubuntu:/etc/openvpn/easy-rsa/2.0# ls
build-ca          build-key-server  list-crl          revoke-full
build-dh          build-key          list-crl          sign-req
build-inter       build-key-pass    openssl-0.9.6.cnf vars
build-key         clean-all        openssl.cnf       whichopensslcnf
build-key-pass    inherit-inter     pkitsol
build-key-pkcs12  keys             README.gz
root@ubuntu:/etc/openvpn/easy-rsa/2.0# adduser longbao01mm03a
Adding user `longbao01mm03a' ...
Adding new group `longbao01mm03a' (1003) ...
Adding new user `longbao01mm03a' (1003) with group `longbao01mm03a' ...
Creating home directory `/home/longbao01mm03a' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for longbao01mm03a
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
root@ubuntu:/etc/openvpn/easy-rsa/2.0# adduser longbao01mm03a
```

Hình 3.7. Tạo và add user

- Tạo key chứng thực cho tài khoản quản trị của server

```
build-key-pkcs12 keys README.gz
root@ubuntu:/etc/openvpn/easy-rsa/2.0# ./build-key-server openvpnserver
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'openvpnserver.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VIETNAM]:
string is too long, it needs to be less than 2 bytes long
Country Name (2 letter code) [VIETNAM]:VN
State or Province Name (full name) [TP DANANG]:
Locality Name (eg, city) [DN]:
Organization Name (eg, company) [VIETHAN]:
Organizational Unit Name (eg, section) []:_
```

Hình 3.8. Tạo key chứng thực cho server

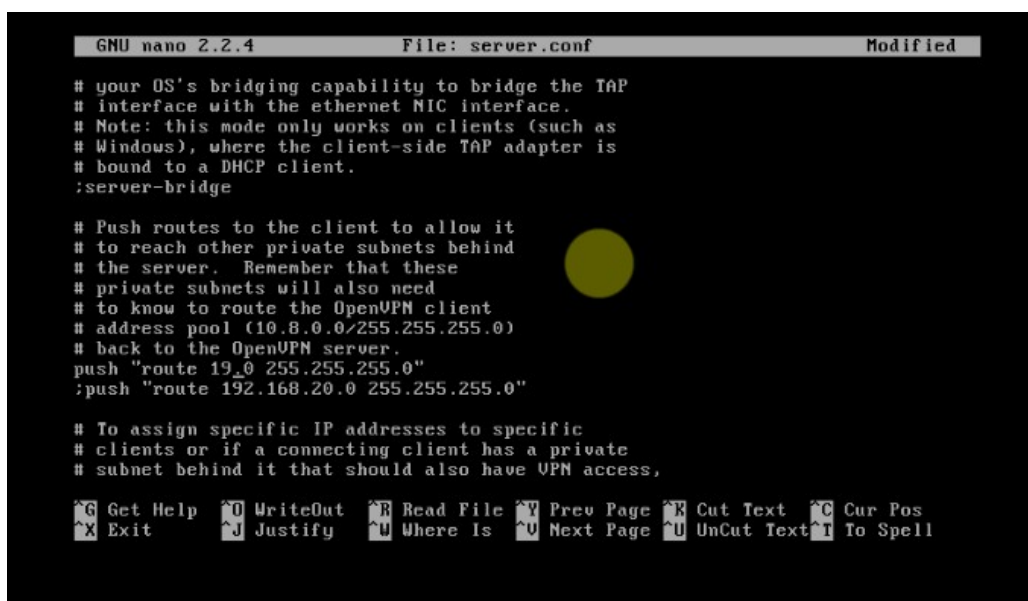
- Tạo key chứng thực cho các user vừa mới tạo ở trên, để các user này có quyền đăng nhập tại máy Client

```
Write out database with 1 new entries
Data Base Updated
root@ubuntu:/etc/openvpn/easy-rsa/2.0# ./build-key longbao02nm03a
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'longbao02nm03a.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VIETNAM]:VN
State or Province Name (full name) [TP DANANG]:
Locality Name (eg, city) [DN]:
Organization Name (eg, company) [VIETHAN]:
Organizational Unit Name (eg, section) []:_
```

Hình 3.9. Tạo key cho các user

➤ Chỉnh sửa thông tin trong file cấu hình như sau

- ca “nhập đường dẫn chứa file ca vừa được build ở trên”.
- Cert “nhập đường dẫn chứa file crt”.
- Key “nhập đường dẫn chứa file key ”
- Các file này thường nằm trong thư mục easy-rsa trên cùng thư mục với openvpn



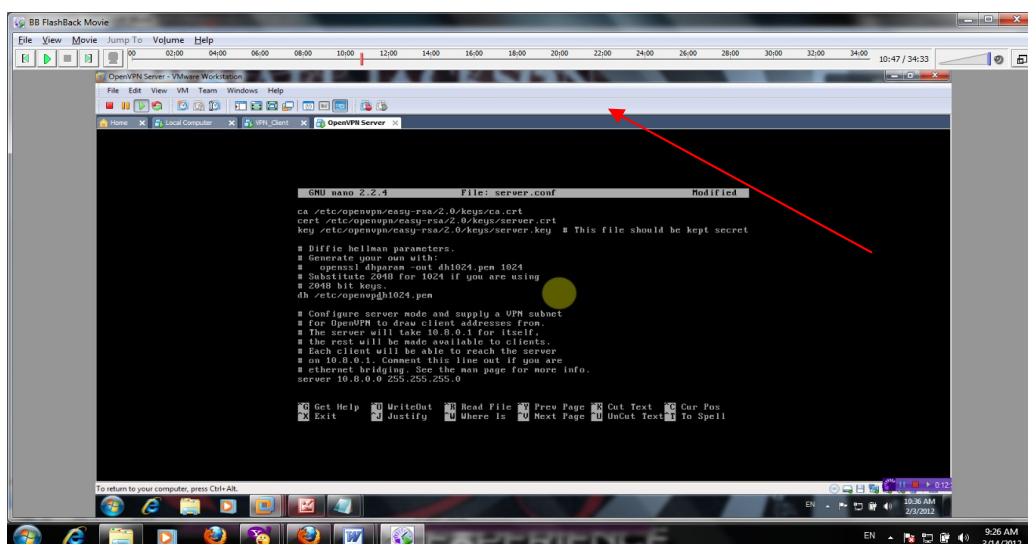
```
GNU nano 2.2.4 File: server.conf Modified

# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
:server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server. Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
push "route 19_0 255.255.255.0"
:push "route 192.168.20.0 255.255.255.0"

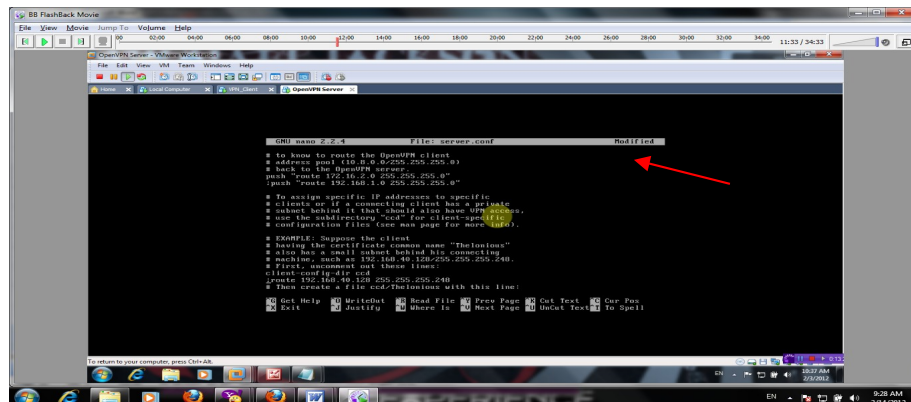
# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
```

Hình 3.10. Cấu hình các thông tin trong file server.conf



Hình 3.11. Chỉnh đường dẫn chứa file chứng thực

- Thực hiện việc thêm các route và miền mạng cần kết nối, để khi khởi động chương trình thì các route này được đẩy tới VPNClient



Hình 3.12. Thêm các route và miền mạng cần kết nối



Hình 3.13. Thực hiện bấm các key để mã hóa

- Tiến hành thực hiện bấm các key mã hóa, để dữ liệu được an toàn khi truyền trên mạng.
- Chỉnh thông số trong file sys để có thể forward gói tin từ client về server và ngược lại.

```
GNU nano 2.2.4 File: /etc/sysctl.conf

# See http://lun.net/articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
```

Hình 3.14. Cấu hình file sysctl.conf và chỉnh ip để forward gói tin

```
GNU nano 2.2.4 File: longbao01nn03a Modified

ifconfig-push 10.8.0.1 10.8.0.2_
```

Hình 3.15. Đẩy IP của VPN vào cho các user để nó tự cấp phát khi kết nối

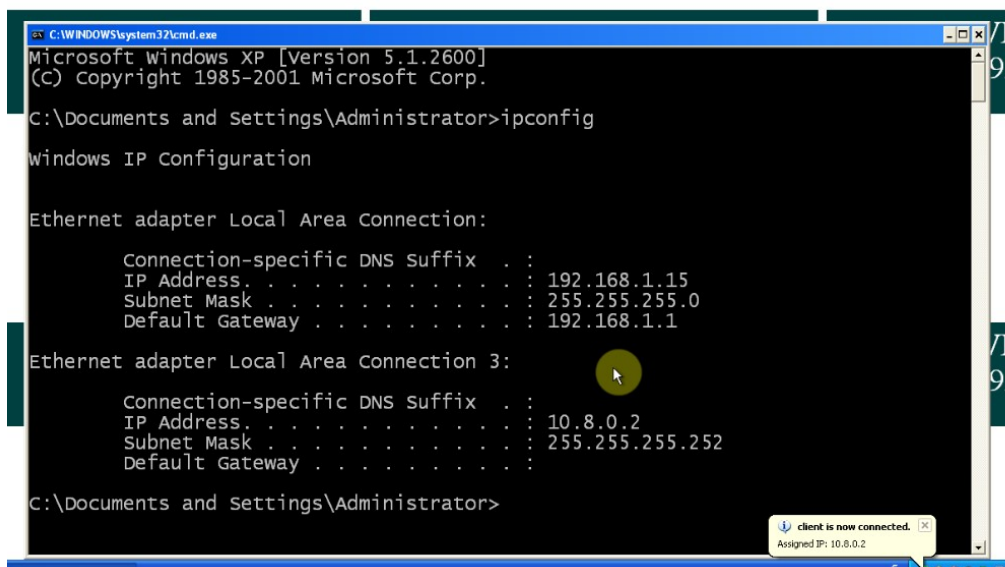
```
longbaoitc@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0
-j MASQUERADE
longbaoitc@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
longbaoitc@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
longbaoitc@ubuntu:~$ sudo iptables -A FORWARD -i tun+ -j ACCEPT
longbaoitc@ubuntu:~$ sudo iptables -A INPUT -i tun+ -j ACCEPT
longbaoitc@ubuntu:~$ sudo iptables -A INPUT -i tap+ -j ACCEPT
longbaoitc@ubuntu:~$ sudo iptables -A FORWARD -i tap+ -j ACCEPT
longbaoitc@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -d 172.1
6.2
```

Hình 3.16. Cấu hình iptables để cho phép forward các gói tin từ VPNClient tới Server

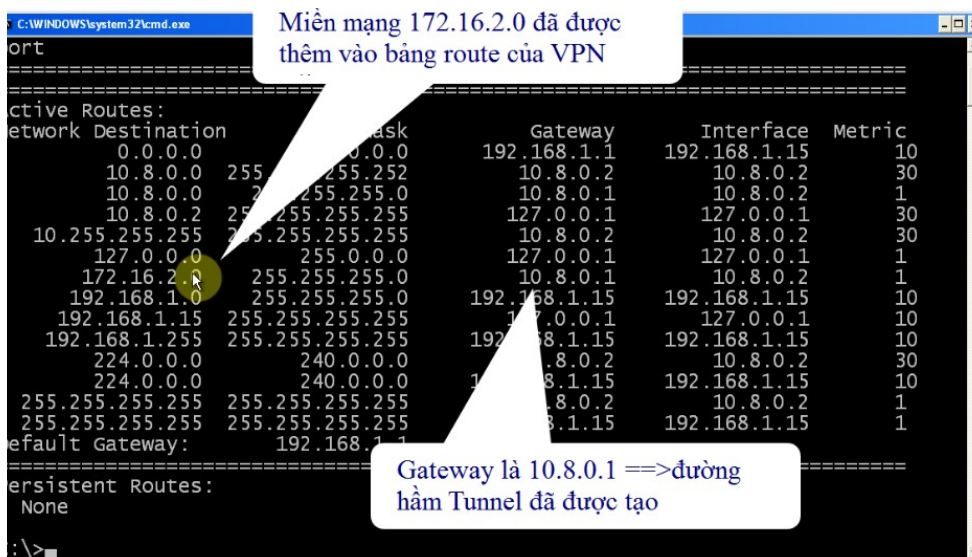
- Add các route của VPN vào user của client cần kết nối bằng cách tạo file với tên các user và đặt trong cùng thư mục openvpn, sau đó tiến hành add các ip của VPN vào các file này.
- Thêm các lệnh iptable để VPNClient có thể truy cập kết nối đến Server

3.3. KIỂM TRA VÀ QUAY KẾT NỐI

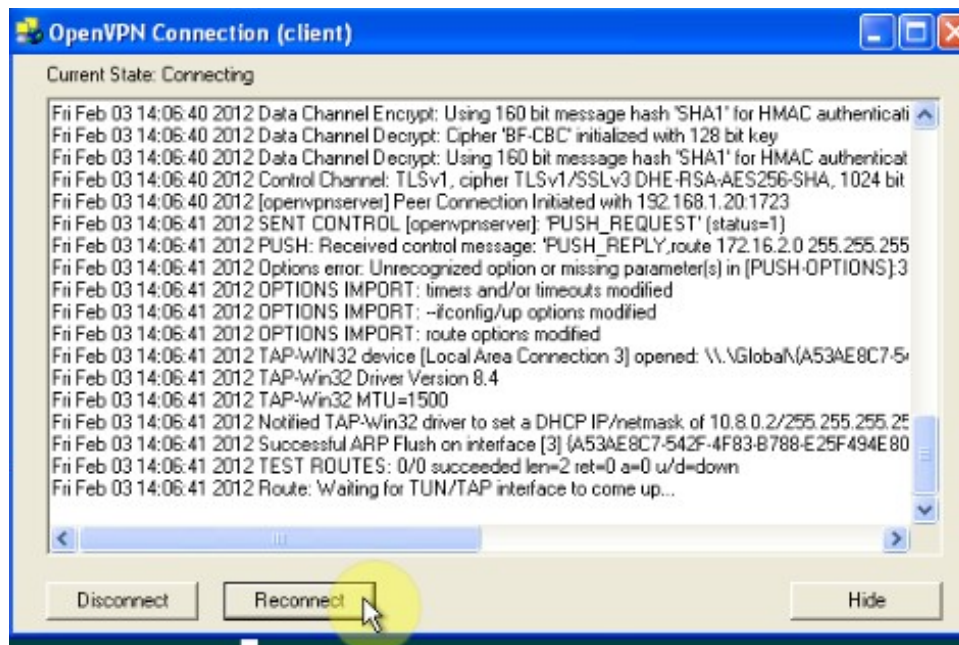
3.3.1. Quay kết nối tại máy VPN Client



Hình 3.17. Quay kết nối thành công tại máy VPN Client

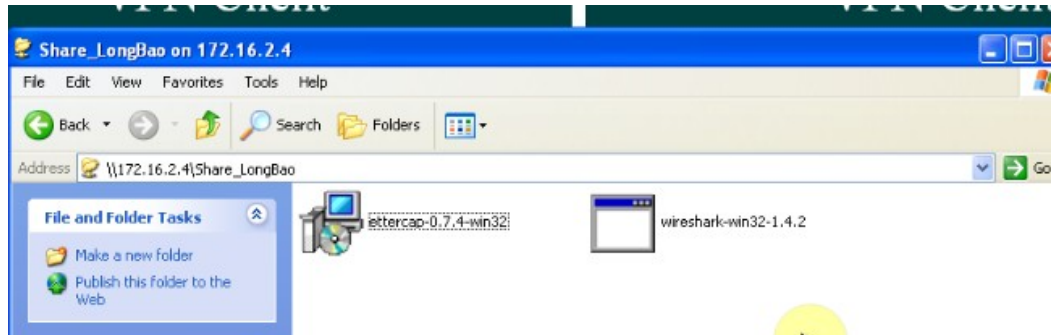


Hình 3.18. Các route đã được add vào thành công



Hình 3.19. Trạng thái của chương trình hoạt động

3.3.2. Kiểm tra lấy thư mục từ Client tới Server



Hình 3.20. Truy cập thư mục mạng nội bộ thành công

KẾT LUẬN

Trong môi trường cạnh tranh và hội nhập như hiện nay, để có thể tồn tại và phát triển thì CNTT là một vũ khí không thể thiếu đối với các doanh nghiệp hiện nay. Vấn đề lợi nhuận, chi phí, giá thành cho các trang thiết bị phục vụ công tác quản trị, hiệu quả, năng suất của công việc, được các doanh nghiệp đặt lên hàng đầu.

Với mô hình kết nối sử dụng máy chủ Linux như Ubuntu Server và phần mềm OpenVPN sẽ giúp các doanh nghiệp đặc biệt là người quản trị mạng có thể quản lý, làm việc từ xa, thông qua các kết nối với các giao thức bảo mật như L2TP, PPTP, IPSec,.... Người dùng có thể truy cập tại nhà hoặc tại các văn phòng chi nhánh của công ty để truy cập kết nối tới công ty làm việc. Với giải pháp nguồn mở và việc sử dụng máy chủ Linux như Ubuntu Server làm máy chủ, sẽ giúp các doanh nghiệp giảm tải gánh nặng về tài chính, các trang thiết bị liên quan, đồng thời tăng cường khả năng bảo mật cho doanh nghiệp.

➤ Kết quả đạt được

○ Về lý thuyết:

Nắm được cơ bản các kiến thức liên quan đến phần mềm nguồn mở, các giải pháp về phần mềm nguồn mở, các phiên bản hệ điều hành Linux như Redhat, Ubuntu,... Cùng với đó nắm được nguyên lý, các giao thức bảo mật liên quan đến kết nối VPN.

○ Về thực hành:

Triển khai thành công ứng dụng phần mềm OpenVPN cho doanh nghiệp với kết nối Client to Site trên môi trường VMWare.

➤ Hạn chế

Do thời gian hạn hẹp, nên chỉ triển khai kết nối Client to Site, chưa triển khai được kết nối Site to Site.

➤ Hướng mở

Tiếp tục triển khai kết nối Site to Site, kết hợp với tìm hiểu các giải pháp bảo mật an toàn hơn cho kết nối VPN như thực hiện chứng thực password một lần (One time password), v...v...

TÀI LIỆU THAM KHẢO

➤ Tài liệu tiếng việt

- [1]. Th.s. Đặng Quang Hiển, *Giáo trình Hệ điều hành Linux*, Trường Cao Đẳng CNTT Hữu Nghị Việt Hàn.
- [2]. Th.s Ngô Bá Hùng, *Giáo trình Linus Operating System*, Trường Đại Học Cần Thơ.
- [3]. Th.s Hà Quốc Trung – Lê Xuân Thành, *Nhập môn Linux và phần mềm nguồn mở*.
- [4]. Đại Học Cần Thơ, *Tìm hiểu phần mềm nguồn mở Open Source Software*.
- [5]. Đại Học Cần Thơ, *Tổng quan về VPN*.
- [6]. Đại Học Quốc Gia TP HCM, *Công nghệ VPN*.

➤ Tài liệu tiếng anh

- [1]. Markus Feilner, *OpenVPN Building and Integrating Virtual Private Networks* (2006).

➤ Internet

- [1]. <http://sourceforge.net/projects/openvpn-gui/>
- [2]. <http://hvaonline.net>
- [3]. <http://nhatnghe.com>
- [4]. <http://quantrimang.com>
- [5]. <http://www.ventanazul.com>

Ý KIẾN GIẢNG VIÊN HƯỚNG DẪN

This image shows a full page of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page, providing a template for handwriting practice or general writing. There are no margins, text, or other markings on the page.