**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 7**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 7: Tìm hiểu và cài đặt, cấu hình máy chủ VPN**

**Họ và tên giảng viên:**

**Thầy :Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

**Cài đặt, cấu hình VPN Server**

**1. Mục đích**

- Tìm hiểu về mạng riêng ảo (VPN-Virtual Private Network), kiến trúc và hoạt động của mạng riêng ảo.

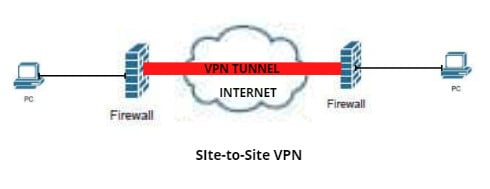
- Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ mạng riêng ảo (VPN server).

**2. Nội dung thực hành**

**2.1 Tìm hiểu lý thuyết**

**2.1.1 Khái quát về VPN, các mô hình VPN và ứng dụng VPN**

- VPN hay còn gọi là Virtual Private Network (mạng riêng ảo), cho phép người dùng thiết lập mạng riêng ảo với một mạng khác trên Internet. VPN có thể được sử dụng để truy cập các trang web bị hạn chế truy cập về mặt địa lý, bảo vệ hoạt động duyệt web khỏi “sự tò mò” trên mạng wifi công cộng bằng cách thiết lập mạng riêng ảo.Muốn kết nối vào hệ thống VPN, thì mỗi tài khoản đều phải được xác thực (phải có Username và Password). Những thông tin xác thực tài khoản này được dùng để cấp quyền truy cập thông qua 1 dữ liệu – Personal Identification Number (PIN), các mã PIN này thường chỉ có tác dụng trong 1 khoảng thời gian nhất định.VPN che dấu địa chỉ giao thức internet (IP) để các hành động trực tuyến của bạn hầu như không thể theo dõi được.



- Công nghệ VPN có thể được phân loại 2 loại cơ bản: Site-to-Site VPN và Remote Access VPN+Site-to-Site VPN hay còn gọi là LAN-to-LAN VPN sử dụng kết nối mạng tunnel mode giữa các Gateway (Gateway có thể là các Router hay Firewall router hỗ trợ VPN).Là mô hình dùng để kết nối các hệ thống mạng ở các nơi khác nhau tạo thành một hệ thống mạng thống nhất. Ở loại kết nối này thì việc chứng thực ban đầu phụ thuộc vào thiết bị đầu cuối ở các Site, các thiết bị này hoạt động như Gateway và đây là nơi đặt nhiều chính sách bảo mật nhằm truyền dữ liệu một cách an toàn giữa các Site.

- Remote Access VPN: 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.Loại này thường áp dụng cho nhân viên làm việc lưu động hay làm việc ở nhà muốn kết nối vào mạng công ty một cách an toàn. Cũng có thể áp dụng cho văn phòng nhỏ ở xa kết nối vào văn phòng trung tâm của công ty. Remote Access VPN còn được xem như là dạng User-to-LAN, cho phép người dùng ở xa dùng phần mềm VPN Client kết nối với VPN Server.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.

- Ưu nhược điểm các VPN

* Ưu điểm: chi phí thiết lập mạng thấp, tăng cường tính bảo mật cho hệ thống...
* Nhược điểm: VPN không có khả năng quản lý Quality of Service (QoS) qua môi trường Internet, do vậy các gói dữ liệu (Data package) vẫn có nguy cơ bị thất lạc, rủi ro. Khả năng quản lý của các đơn vị cung cấp VPN là có hạn nên máy tính vẫn có thể bị hack, tiềm ẩn nguy cơ bảo mật cho máy tính.

- Ứng dụng của VPN

* Truy cập vào mạng doanh nghiệp khi ở xa
* Truy cập vào mạng gia đình,dù không ở nhà − Duyệt web ẩn danh
* Truy cập vào những website bị chặn giới hạn địa lý − Tải tập tin

**2.1.2 Các giao thức tạo đường hầm choVPN: PPTP, L2TP, MPLS...**

**a. Giao thức PPTP**

- PPTP (Point-to-Point Tunneling Protocol-giao thức đường hầm điểm nối điểm) là giao thức được dùng để truyền dữ liệu qua các hầm -Tunnel giữa 2 tầng traffic trong Internet.PPTP được coi là phương thức đào đường hầm kém an toàn nhất, cũng là giao thức lâuđời nhất trong số các giao thức. Nó được tạo bởi Microsoft và phát hành cùng Windows 95. Tất cả những gì bạn cần là tên người dùng và mật khẩu với địa chỉ máy chủ để thực hiện kết nối. PPTP cũng là giao thức VPN Tunneling nhanh nhất vì mức độ mã hóa của nó quá thấp. Nếu không quan tâm về bảo mật, lựa chọn này có thể phù hợp về tốc độ.

**b. Giao thức L2TP**

- L2TP (Layer 2 Tunneling Protocol) là mạng riêng ảo được phát triển bởi Microsoft và Cisco.L2TP tốt hơn PPTP về mặt bảo mật nhưng về tốc độ thì PPTP nhanh hơn, nó không có mã hóa riêng. Dữ liệu và lưu lượng đi qua đường hầm này thường được mã hóa bằng giao thức bảo mật IPSec. L2TP/IPSec cung cấp cho người dùng công nghệ mã hóa tiên tiến nhất, AES-256. L2TP là một giao thức phổ biến vì mức độ bảo mật cao nhưng nó không thể vượt qua một số tường lửa hạn chế vì nó sử dụng các cổng cố định để kết nối.

**c. Giao thức MPLS**

- MPLS (Multi Protocol Label Switching) là công nghệ chuyển mạch nhãn đa giao thức,một tập các công nghệ mở dựa vào chuẩn Internet mà kết hợp chuyển mạch lớp 2 và định tuyến lớp 3 để chuyển tiếp gói tin bằng cách sử dụng các nhãn ngắn có chiều dài cố định. MPLS cho phép các ISP hợp nhất các mạng sử dụng các công nghệ khác nhau vào trong một mạng duy nhất, và đặc biệt quan trọng là cho các nhà ISP đạt được việc điều khiển lưu lượng một cách chính xác tại lớp IP.Bằng cách sử dụng các giao thức điều khiển và định tuyến Internet, MPLS cung cấp chuyển mạch hướng kết nối ảo qua các tuyến Internet bằng cách sử dụng các nhãn và trao đổi nhãn. MPLS bao gồmviệc thực hiện các đường chuyển mạch nhãn LSP, nó cũng cung cấp các thủ tục và các giao thức cần thiết để phân phối các nhãn giữa các chuyển mạch và các bộ định tuyến.

**2.1.3 Các giao thức bảo mật cho VPN: IPSec, SSL/TLS**

**a. IPSec**

- IPSec (IP Security) là một tập các giao thức chuẩn, cung cấp các dịch vụ bảo mật cho những gói tin IP tại lớp network. Những dịch vụ này bao gồm các điều khiển truy cập (access control list), toàn vẹn dữ liệu (data integrity), xác thực (authentication), tránh trùng lặp gói tin (against replay) và sự bảo mật dữ liệu (data security).Mục đích chính của IPSec là bảo vệ luồng dữ liệu mong muốn dựa trên các dịch vụ bảo mật có sẵn.IPSec là sự lựa chọn hàng đầu cho việc bảo mật VPN.

**b. SSL/TSL**

- SSLlà chữ viết tắt củaSecure Sockets Layer (Lớp socket bảo mật). Một loại bảo mật giúp mã hóa liên lạc giữa website và trình duyệt. Công nghệ này đanglỗi thờivà được thay thế hoàn toàn bởiTLS. TLSlà chữ viết tắt củaTransport Layer Security,nó cũng giúp bảo mật thông tin truyền giống như SSL. Website được càiđặt chứng chỉ SSL/TLS có thể dùng gaio thức HTTPS để thiết lập kênh kết nối an toàn tới server. Mục tiêu của SSL/TLS là bảo mật các thông tin nhạy cảm trong quá trình truyền trên internet như, thông tin cá nhân, thông tin thanh toán, thông tin đăng nhập. Nó là giải pháp thay thế cho

phướng pháp truyền thông tin văn bản dạng plain text, văn bản loại này khi truyền trên internet sẽ không được mã hóa, nên việc áp dụng mã hóa vào sẽ khiến cho các bên thứ 3 không xâm nhập được bào thông tin của bạn, không đánh cắp hay chỉnh sửa được các thông tin đó.Chứng chỉ SSL/TLS hoạt động bằng cách tích hợp key mã hóa vào thông tin định danh công ty. Nó sẽ giúp công ty mã hóa mọi thông tin được truyền mà không bị ảnh hưởng hoặc chỉnh sửa bởi các bên thứ 3. SSL/TLS hoạt động bằng cách sử dụng public và private key, đồng thời các khóa duy nhất của mỗi phiên giao dịch. Mỗi khi khách truy cập điền vào thanh địa chỉ SSL thông tin web browser hoặc chuyển hướng tới

trang web được bảo mật, trình duyệt và web server đã thiết lập kết nối. Trong phiên kết nối ban đầu, public và private key được dùng để tạo session key, vốn được dùng để mã hóa và giải mã dữ liệu được truyền đưa. Session key sẽ được sử dụng trong một khoảng thời gian nhất định và chỉ có thể dùng cho phiên giao dịch này.

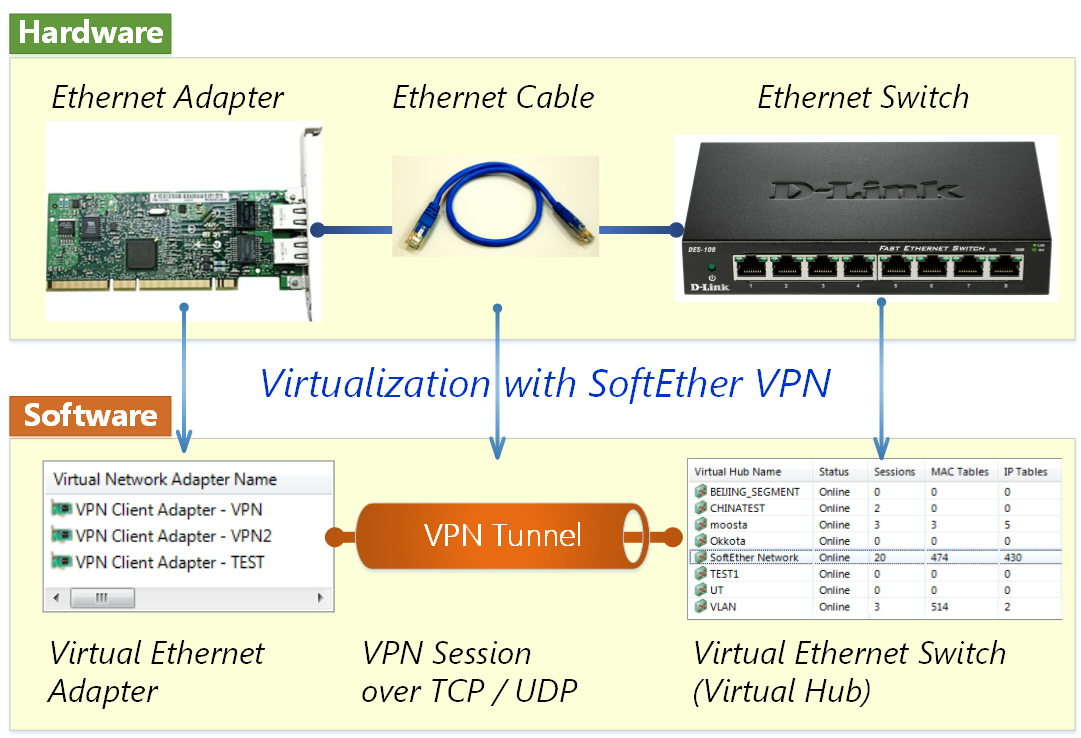
**2.1.4 SoftEther VPN**

- Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và BẢO MẬT cao hơn. SoftEther VPN khởi đầu là một dự án học thuật tại Đại học Tsukuba và là một Phần mềm VPN đa giao thức đa nền tảng mã nguồn mở miễn phí. Hiện tại, SoftEther VPN hỗ trợWindows, Linux, Mac, Solaris, FreeBSDvà thường là một lựa chọn tốt để thay thế cho OpenVPN vì nhanh hơn. Bên cạnh đó, SoftEther VPN còn sử dụngkey certificate AES 256 bit,,1 cấp độ bảo mật và mã hóa cao. Thêm một điểm cộng lớn cho phần mềm này là nó tích hợp tất cả các tính năng của các giao thức VPN khác nhau như PPTP, L2TP, OpenVPN và SSTP, trong khi loại bỏ nhược điểm của chúng. Tất cả các tính năng mà SoftEthercung cấp, tăng cường khả năng giúp người dùng điều hướng an toàn và vượt qua mọi tường lửa do các bên chính quyền áp đặt, giúp nó trở thành một giao thức VPN phổ biến

- Các tính năng của SoftEther VPN:

* Phần mềm miễn phí và mã nguồn mở.
* Dễ dàng thiết lập cảVPN truy cập từ xa và vpn từ trang web đến trang web.
* Ssl-VPN Đường hầm trên HTTPS để đi qua NATs và tường lửa. +VPN mang tính cách mạng qua ICMP và VPN qua các tính năng DNS.
* Khả năng chống lại tường lửa bị hạn chế cao.
* Đủ tính năng bảo mật như ghi nhật ký và tường lửa bên trong đường hầm VPN.
* Mã hóa AES 256-bit và RSA 4096-bit.

- Kiến trúc của SoftEther VPN:Chuẩn bị máy kali



Máy Kali

Text

Description automatically generated

Máy Windows

Text

Description automatically generated

Text

Description automatically generated

Cài đặt GCC

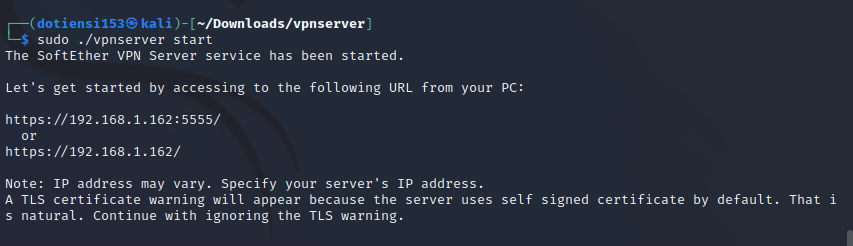
Text

Description automatically generated

Text

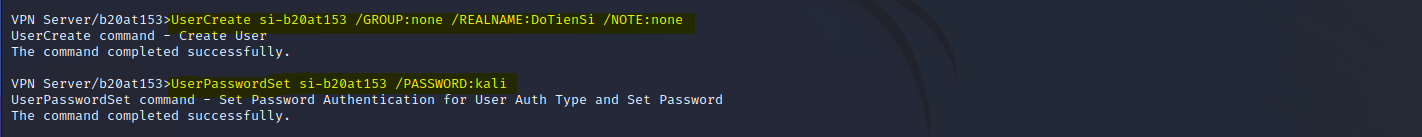
Description automatically generated

Khởi động máy chủ VPN: **sudo ./vpnserver start**



Tạo 1 vitual hub và tạo 1 người dùng mới

Text

Description automatically generated 

Tải SoftEther VPN server trên máy Linux

Graphical user interface, text, application

Description automatically generated

Tạo và kiểm tra kết nối VPN

Calendar

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated Table

Description automatically generated with medium confidence

sudo grep<mã sinh viên> vpnserver/server\_log/\*.logA picture containing graphical user interface

Description automatically generated