**BÁO CÁO ĐỒ ÁN**

**AN TOÀN MÁY CHỦ WINDOWS**



**Đề tài: Tìm hiểu và triển khai giao thức SSTP VPN**

Giảng viên hướng dẫn**:**

Lớp**:**

Sinh viên thực hiện:

|  |  |
| --- | --- |
|  |  |

Thành phố Hồ Chí Minh, năm 2022

**LỜI MỞ ĐẦU**

Công nghệ thông tin là một trong những ngành đang rất được trọng dụng trong những năm gần đây, với sự tác động mạnh mẽ của cách mạng công nghệp 4.0 ngành công nghệ thông tin đang là mối quan tâm hàng đầu trong bước tiến mới của thời đại công nghệ hóa đang dần thay thế phần lớn công việc của con người. Thế nên ở các nước đang đẩy mạnh đào tạo ra các nguồn nhân lực Công nghệ thông tin nhằm đáp ứng nhu cầu việc làm mà xã hội cần thiết để đảm bảo nguồn nhân lực cho sự phát triển của thời đại công nghệ này.

Trong các doanh nghiệp, đối với những người dùng có nhu cầu kết nối từ xa để truy cập mạng nội bộ, người quản trị thường cấu hình Virtual Private Network (VPN) cho phép người dung có thể kết nối vào mạng nội bộ từ một máy Client nào đó thông qua đường truyền Internet công cộng. Kỹ thuật VPN thông thường sử dụng Point to Point Tunneling Protocol (PPTP) hoặc Layer two Tunnneling Protocol (L2TP) kết hợp IPSEC. Tuy nhiên trong trường hợp người dùng ngồi trên 1 Client thuộc một mạng nội bộ khác truy cập Internet thông qua một Firewall, Firewall này không cho phép thiết lập kết nối PPTP hoặc L2TP thì người dùng sẽ không thể kết nối VPN vào mạng doanh nghiệp. Giải pháp trong tình huống này là sử dụng Secure Socket Tunneling Protocol (SSTP).

SSTP được giới thiệu từ Windows Server 2008 cho phép thiết lập kết nối VPN thông qua kênh mã hóa SSL của HTTPS, có nghĩa là kết nối sẽ chạy port 443, trong trường hợp này có thể thông qua các firewall cho phép truy cập Web.

Trong bài viết này sẽ giới thiệu kỹ thuật kết nối VPN bằng SSTP trong môi trường Windows Server 2012

**Chương 1: Tổng quan**

**1.1. Tổng quan đề tài**

1.1.1 Khảo sát thực trạng

Là một trong những công nghệ được sử dụng nhiều nhất hiện nay vì lý do bảo mật, kết nối và sử dụng đơn giản là VPN (Mạng riêng ảo - Mạng riêng ảo), nhờ thiết kế của nó, 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 vị trí địa lý, bảo vệ hoạt động duyệt web của bạn khỏi “sự tò mò” trên mạng Wifi công cộng bằng cách [thiết lập mạng riêng ảo](https://thuthuat.taimienphi.vn/cach-thiet-lap-mang-ca-nhan-ao-cach-cai-mang-ca-nhan-ao-21950n.aspx) cho bạn, ….

1.1.2 Đánh giá

**- Ưu điểm của VPN**

**+ Ẩn danh tính trực tuyến**

**+ VPN giúp bạn vượt qua khoảng cách địa lý**

**+ VPN bảo mật các kết nối trực tuyến**

**+ VPN có thể ngăn chặn việc điều chỉnh băng thông**

**+ VPN có thể vượt tường lửa**

**- Nhược điểm của VPN**

**+ VPN đôi khi làm chậm tốc độ truy cập internet**

**+ Sử dụng VPN sai có thể khiến quyền riêng tư của bạn gặp nguy hiểm**

**+ VPN chất tượng sẽ khá tốn tiền**

**+ Không phải tất cả các thiết bị đều hỗ trợ VPN**

**1.2. Mục tiêu**

- Nghiên cứu, tìm hiểu các chức năng, hoạt động của VPN và SSTP

- Nghiên cứu cách thức hoạt động, các yêu cầu, công nghệ sử dụng dịch vụ.

- Nghiên cứu cách cài đặt các dịch vụ bảo mật

- Nâng cao tầm hiểu biết và mở rộng kiến thức

- Rèn luyện kỹ năng làm việc nhóm, cách triển khai của một dự án

- Học hỏi những công nghệ mới, áp dụng công nghệ vào một dự án cụ thể

**1.3. Cấu trúc đề tài**

Đồ án được chia làm 4 phần tương ứng với 4 chương:

Chương 1: Tổng quan

+ Tổng quan đề tài

+ Mục tiêu

+ Cấu trúc đề tài

Chương 2: Cơ sở lý thuyết

Chương 3: Kết quả thực nghiệm

+ Kịch bản thực nghiệm

+ Yêu cầu thực nghiệm

+ Công cụ sử dụng

+ Các bước thực hiện

+ Kết luận

Chương 4: Kết luận và hướng phát triển

**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT**

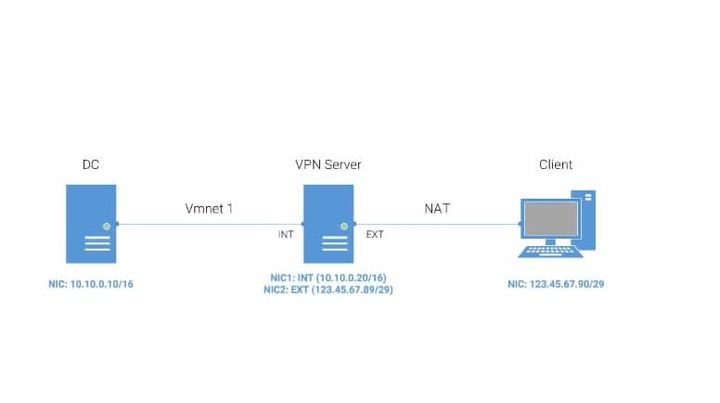
**2.1. Giới thiệu về SSTP và VPN**

SSTP, hay Secure Socket Tunneling Protocol, được thiết kế để bảo vệ lưu lượng PPP bằng cách sử dụng kênh SSL/TLS. SSTP tốt và an toàn hơn nhiều cho người dùng Windows so với L2TP/IPSec hoặc [PPTP](https://quantrimang.com/point-to-point-tunneling-protocol-la-gi-174003). SSTP rất khó để chặn và chỉ cung cấp tốc độ tốt nếu bạn có đủ băng thông.

## SSTP (Secure Socket Tunneling Protocol) là gì?

Viết tắt của Secure Socket Tunneling Protocol, SSTP là một loại [VPN tunnel](https://quantrimang.com/vpn-tunnel-la-gi-174006) sử dụng kênh SSL 3.0 để gửi lưu lượng PPP hoặc L2TP. SSL cho phép truyền tải và mã hóa dữ liệu, cũng như kiểm tra tính toàn vẹn của lưu lượng. Do đó, SSTP có thể vượt qua hầu hết các tường lửa và [proxy server](https://quantrimang.com/ly-thuyet-proxy-la-gi-117220) bằng cách sử dụng kênh SSL qua [cổng TCP 443](https://quantrimang.com/cong-443-la-gi-174256).

SSTP có sẵn để sử dụng trong môi trường Windows (kể từ Windows Vista SP1), trong RouterOS và trong SEIL (kể từ phiên bản firmware 3.50). SSTP có thể được sử dụng với Winlogon hoặc xác thực thẻ thông minh, các chính sách truy cập từ xa và Windows VPN client, vì được tích hợp với kiến trúc RRAS.

Như với các giao thức tunneling IP-over-TCP khác, SSTP chỉ hoạt động tốt nếu có đủ băng thông trên liên kết mạng không được tạo tunnel. Nếu không có đủ băng thông, TCP timer (công cụ được sử dụng bởi TCP để tránh sự chậm trễ quá mức trong quá trình giao tiếp) có thể sẽ hết hạn, gây ra sự sụt giảm lớn về hiệu suất SSTP.

## SSTP hoạt động như thế nào?

Hệ thống của client kết nối với máy chủ thông qua TCP (Transmission Control Port). SSL sử dụng cổng 443 để kết nối với máy chủ. Để xác nhận kết nối, nó yêu cầu xác thực người dùng và thường được xác thực bởi client. Giao thức sử dụng chứng chỉ máy chủ để xác thực.

## Tại sao SSTP là một giao thức VPN phổ biến?

Có nhiều lý do chứng thực sự phổ biến của SSTP. Ví dụ, SSTP cung cấp mức bảo mật cao nhất, tức là mã hóa AES 256-bit. Hơn nữa, cổng nó sử dụng có thể né tránh hầu hết các loại [tường lửa](https://quantrimang.com/tong-quan-ve-firewall-84474). Vì SSTP là tài sản thuộc sở hữu của Microsoft nên nó hoàn toàn tương thích với Windows.

SSTP là một giao thức VPN phổ biến

## Ưu và nhược điểm của SSTP

### **Ưu điểm**

Có khả năng vượt qua đa số các loại tường lửa.

Mức độ bảo mật lệ thuộc vào mật mã, nhưng nó thường được bảo mật.

Được bổ trợ bởi Microsoft & tích hợp vào hệ điều hành Windows.

### **Nhược điểm**

Vì này là gia tài của Microsoft nên không bên thứ ba nào có thể kiểm tra lỗ hổng bảo mật.  
Tốc độ chậm do chừng độ mã hóa cao.

## 2.2 Mạng riêng ảo VPN là gì?

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

1 hệ thống VPN có thể kết nối được nhiều site khác nhau, dựa trên khu vực, diện tích địa lý… tượng tự như chuẩn **Wide Area Network (WAN)**. Bên cạnh đó, VPN còn được dùng để “khuếch tán”, mở rộng các mô hình Intranet nhằm truyền tải thông tin, dữ liệu tốt hơn. Ví dụ, các trường học vẫn phải dùng VPN để nối giữa các khuôn viên của trường (hoặc giữa các chi nhánh với trụ sở chính) lại với nhau.

Nếu muốn kết nối vào hệ thống VPN, thì mỗi 1 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 (30s hoặc 1 phút).

Khi kết nối máy tính hoặc một thiết bị khác chẳng hạn như điện thoại, máy tính bảng với một VPN, máy tính hoạt động giống như nó nằm trên cùng mạng nội bộ với VPN. Tất cả traffic trên mạng được gửi qua kết nối an toàn đến VPN. Nhờ đó, bạn có thể truy cập an toàn đến các tài nguyên mạng nội bộ ngay cả khi đang ở rất xa.

Bạn cũng có thể sử dụng Internet giống như đang ở vị trí của của VPN, điều này mang lại một số lợi ích khi sử dụng WiFi public hoặc truy cập trang web bị chặn, giới hạn địa lý.

Khi duyệt web với VPN, máy tính sẽ liên hệ với trang web thông qua kết nối VPN được mã hóa. Mọi yêu cầu, thông tin, dữ liệu trao đổi giữa bạn và website sẽ được truyền đi trong một kết nối an toàn. Nếu sử dụng VPN tại Hoa Kỳ để truy cập vào Netflix, Netflix sẽ thấy kết nối của bạn đến từ Hoa Kỳ.

Dù nghe có vẻ khá đơn giản, nhưng trên thực tế VPN lại được ứng dụng để làm rất nhiều thứ:

* **Truy cập vào mạng doanh nghiệp khi ở xa:** VPN thường được sử dụng bởi những người kinh doanh để truy cập vào mạng lưới kinh doanh của họ, bao gồm tất cả tài nguyên trên mạng cục bộ, trong khi đang đi trên đường, đi du lịch,… Các nguồn lực trong mạng nội bộ không cần phải tiếp xúc trực tiếp với Internet, nhờ đó làm tăng tính bảo mật.
* **Truy cập mạng gia đình, dù không ở nhà:** Bạn có thể thiết lập VPN riêng để truy cập khi không ở nhà. Thao tác này sẽ cho phép truy cập Windows từ xa thông qua Internet, sử dụng tập tin được chia sẻ trong mạng nội bộ, chơi game trên máy tính qua Internet giống như đang ở trong cùng mạng LAN.
* **Duyệt web ẩn danh:** Nếu đang sử dụng WiFi công cộng, duyệt web trên những trang web không phải https, thì tính an toàn của dữ liệu trao đổi trong mạng sẽ dễ bị lộ. Nếu muốn ẩn hoạt động duyệt web của mình để dữ liệu được bảo mật hơn thì bạn nên kết nối VPN. Mọi thông tin truyền qua mạng lúc này sẽ được mã hóa.
* **Truy cập đến những website bị chặn giới hạn địa lý,** bỏ qua kiểm duyệt Internet, vượt tường lửa,…
* **Tải tập tin:** Tải BitTorrent trên VPN sẽ giúp tăng tốc độ tải file. Điều này cũng có ích với các traffic mà ISP của bạn có thể gây trở ngại.



## Các giao thức thường dùng trong VPN

Các sản phẩm VPN thường co sự tiện lợi, tính hiệu quả và bảo mật rất đa dạng. Nếu bảo mật là một mối quan tâm hàng đầu, thì một tổ chức cần phải chú ý đến các giao thức mà dịch vụ VPN hỗ trợ. Một số giao thức được sử dụng rộng rãi có những điểm yếu đáng quan ngại, trong khi những giao thức khác lại cung cấp khả năng bảo mật tiên tiến nhất. Những giao thức tốt nhất hiện nay là OpenVPN và IKEv2.

### Tìm hiểu về các giao thức VPN

Bản chất của giao thức VPN là một tập hợp các giao thức. Có một số chức năng mà mọi VPN phải giải quyết được:

– **Tunnelling** (kỹ thuật truyền dữ liệu qua nhiều mạng có giao thức khác nhau) – Chức năng cơ bản của VPN là phân phối các gói (packet) từ điểm này đến điểm khác mà không để lộ chúng cho bất kỳ ai trên đường truyền. Để làm điều này, VPN đóng gói tất cả dữ liệu theo định dạng mà cả máy khách và máy chủ đều hiểu được. Bên gửi dữ liệu đặt nó vào định dạng tunnelling và bên nhận trích xuất để có được thông tin.

– **Mã hóa**: Tunnelling không cung cấp tính năng bảo vệ. Bất cứ ai cũng có thể trích xuất dữ liệu. Dữ liệu cũng cần phải được mã hóa trên đường truyền. Bên nhận sẽ biết cách giải mã dữ liệu từ một người gửi nhất định.

– **Xác thực**. Để bảo mật, VPN phải xác nhận danh tính của bất kỳ client nào cố gắng “giao tiếp” với nó. Client cần xác nhận rằng nó đã đến đúng máy chủ dự định.

– **Quản lý phiên**: Một khi người dùng được xác thực, VPN cần duy trì phiên để client có thể tiếp tục “giao tiếp” với nó trong một khoảng thời gian.

Nói chung các giao thức VPN coi việc tạo tunnel, xác thực và quản lý phiên như một gói. Điểm yếu trong bất kỳ chức năng nào đều là những lỗ hổng bảo mật tiềm ẩn trong giao thức. Mã hóa là một chuyên ngành, nó cũng rất khó, nên thay vì cố gắng tạo ra cái mới, các VPN thường sử dụng kết hợp nhiều giao thức mã hóa đáng tin cậy. Dưới đây là những giao thức VPN phổ biến và độ mạnh yếu của chúng.

## 

## CHƯƠNG 3 : KẾT QUẢ THỰC NGHIỆM

3.1. Kịch bản thực nghiệm

## Cài đặt Enterprise CA

## Tạo Certificate Template và phát hành Certificate Template

## Xin SSTP Certificate cho VPN Server

## Cài đặt Remote Access

## Cấu hình VPN Client-to-Gateway

## Cấu hình NAT Inbound

## Download CA Certificate

## Cấu hình Trusted Root CA trên VPN Client

## Tạo VPN Connection

## Kiểm tra kết nối VPN-SSTP

## 3.3 Công cụ thực hiện :

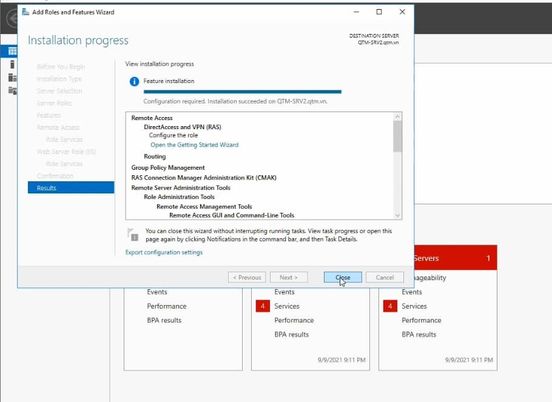
## Download VMware Workstation Pro | ASEAN- Vmware : ****Vmware Work Station**** là sản phẩm đầu tiên được phát hành bởi công ty ****WMware****. Đây là công cụ cho phép người dùng tạo và sử dụng máy ảo trực tiếp trên laptop hoặc PC. Bên cạnh việc cho phép cài đặt nhiều phiên bản hệ điều hành khác nhau, bạn cũng có thể dễ dàng chuyển đổi máy ảo cùng một lúc.

## - Windows server 2016 : Windows Server 2016là một hệ thống điều hành máy chủ được [Microsoft](https://vi.wikipedia.org/wiki/Microsoft) phát triển như là một phần của gia đình hệ điều hành Windows NT, phát triển đồng thời với Windows 10. Phiên bản preview đầu tiên (kỹ thuật trước) đã được đưa ra ngày 01 tháng 10 năm 2014 cùng với các phiên bản preview đầu tiên của [System Center](https://vi.wikipedia.org/w/index.php?title=System_Center&action=edit&redlink=1). Không giống như các phiên bản Windows Server trước, được phát hành đồng thời với hệ thống điều hành máy khách, Windows Server 2016 đã được phát hành vào ngày 26 tháng 9 năm 2016 tại hội nghị Ignite của Microsoft và được đưa ra thị trường vào ngày 12 tháng 10 năm 2016.

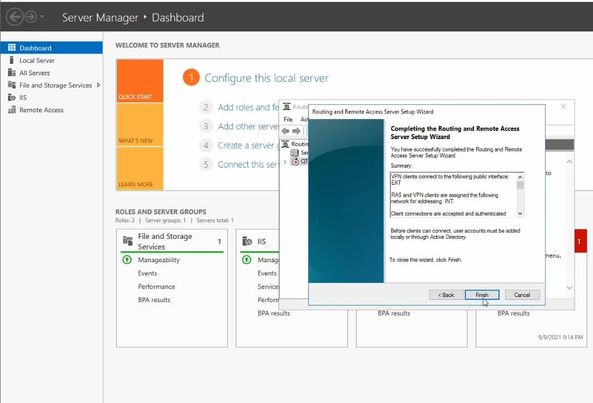
## 3.4 Các bước thực hiện :

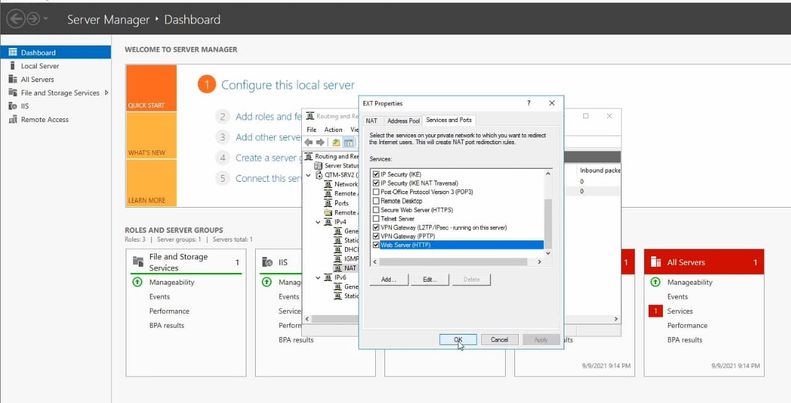
## Mở ảnhBước 1 : Tạo và cấp quyền VPN cho người dung :

## Không có mô tả.Bước 2 : Cài đặt và cấu hình CA

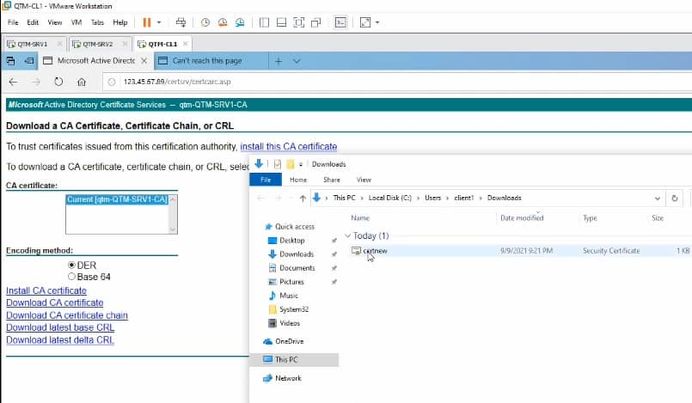
Bước 3 Cài đặt dịch RAS

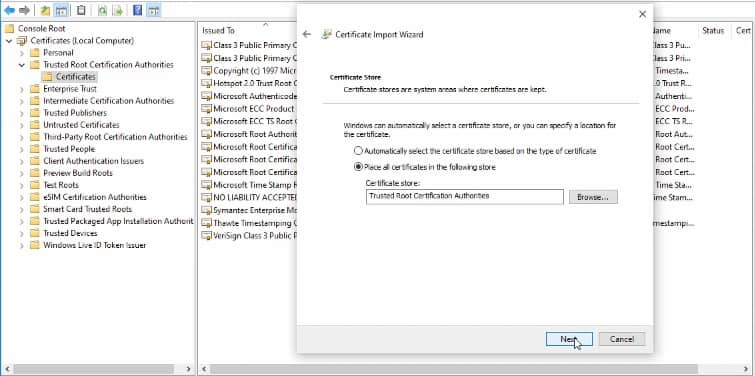
Bước 4 : Cấu hình VPN và NAT



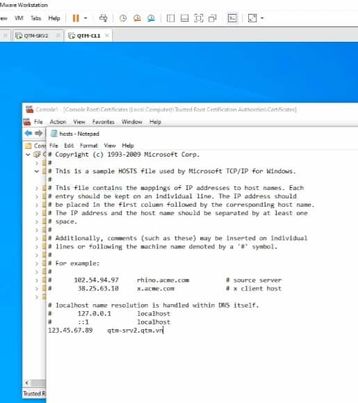
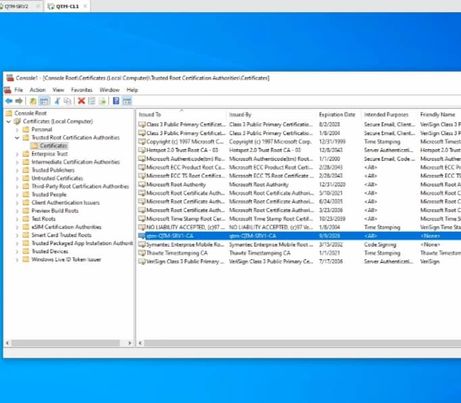


Bước 5: Thực hiện máy trạm:

5.1 Download chứng chỉ và thêm chứng chỉ vào khay Trusted

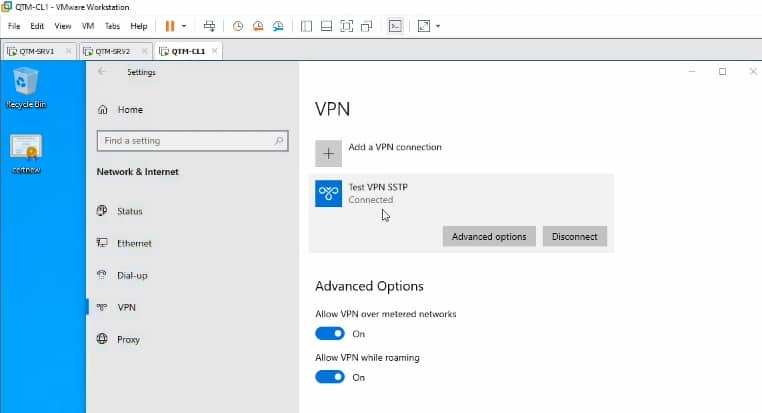


5.2 Thay đổi thông tin của file hosts :

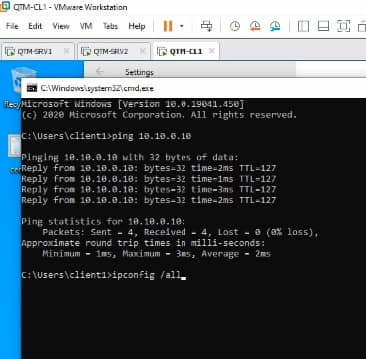


5.3 Tạo kết nối VPN :





Bước 6 kiểm tra kết nối SSTP VPN



**CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

4.1. Kết luận

Secure Socket Tunneling Protocol được giới thiệu trong Windows Vista Service Pack 1. Đây là giao thức Microsoft độc quyền và được hỗ trợ tốt nhất trên Windows. Nó có thể ổn định hơn trên Windows vì nó được tích hợp vào hệ điều hành trong khi OpenVPN thì không - đó là lợi thế tiềm năng lớn nhất. Một số hỗ trợ cho nó có sẵn trên các hệ điều hành khác, nhưng nó gần như không phổ biến rộng rãi.

Nó có thể được cấu hình để sử dụng mã hóa AES rất an toàn, điều này rất tốt. Đối với người dùng Windows, nó chắc chắn tốt hơn PPTP - nhưng, vì nó là một giao thức độc quyền, nó không phụ thuộc vào các kiểm toán độc lập OpenVPN phải chịu. Bởi vì nó sử dụng SSL v3 như OpenVPN, nó có khả năng tương tự để bỏ qua tường lửa và nên hoạt động tốt hơn cho điều này so với L2TP / IPsec hoặc PPTP.