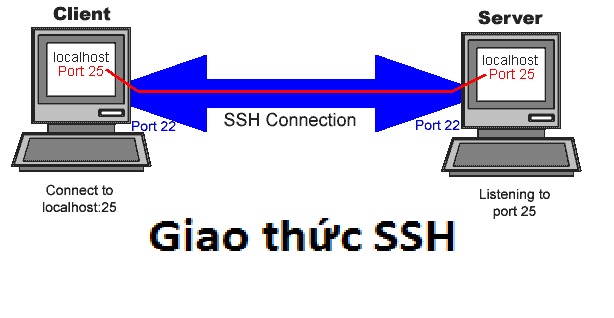
Báo cáo tìm hiểu về SSH

[**SSH là gì?**](https://hostingviet.vn/ssh-la-gi)  
SSH là chữ viết tắt của Secure Shell, tạm dịch là "môi trường an toàn" SSH được hiểu đơn giản là giao thức kết nối giữa máy chủ và máy khách được bảo mật một cách an toàn. Hiểu đơn giản hơn, Bạn sử dụng SSH để kết nối với VPS, Server thì sẽ không sợ bị đánh cắp thông tin được truyền đi giữa máy tính của Bạn và máy chủ. SSH cũng giống như giao thức SSL, nó mã hóa dữ liệu đường truyền. Bạn có thể sử dụng để chạy chương trình, chuyển tập tin, chuyển tiếp khác kết nối TCP / IP qua liên kết an toàn. Hiện nay SSH có phiên bản 2 là SSH2.

**Các công cụ SSH phổ biến hiện nay:** [PuTTY](https://hostingviet.vn/putty-la-gi-cach-su-dung-phan-mem-putty), OpenSSH, Bitvise SSH

[](https://hostingviet.vn/ssh-la-gi)

[**Cách hoạt động của SSH**](https://hostingviet.vn/ssh-la-gi)  
SSH làm việc thông qua 3 bước đơn giản:  
• Định danh host - xác định định danh của hệ thống tham gia phiên làm việc SSH.  
• Mã hoá - thiết lập kênh làm việc mã hoá.  
• Chứng thực - xác thực người sử dụng có quyền đăng nhập hệ thống

***Định danh host (được hiểu là máy khách - máy tính điều khiển)***

Việc định danh host được thực hiện qua việc trao đổi khoá. Mỗi máy tính điều khiển SSH có một khoá định danh duy nhất. Khoá này gồm hai thành phần: khoá riêng tư và khoá công cộng. Khoá công cộng được sử dụng khi cần trao đổi giữa các máy chủ với nhau trong phiên làm việc SSH, dữ liệu sẽ được mã hoá bằng khoá công khai và chỉ có thể giải mã bằng khoá riêng. Khi có sự thay đổi về cấu hình trên máy chủ: thay đổi chương trình SSH, thay đổi cơ bản trong hệ điều hành, khoá định danh cũng sẽ thay đổi. Khi đó mọi người sử dụng SSH để đăng nhập vào máy chủ này đều được cảnh báo về sự thay đổi này. Khi hai hệ thống bắt đầu một phiên làm việc SSH, máy chủ sẽ gửi khoá công cộng của nó cho máy khách. Máy khách sinh ra một khoá phiên ngẫu nhiên và mã hoá khoá này bằng khoá công cộng của máy chủ, sau đó gửi lại cho máy chủ. Máy chủ sẽ giải mã khoá phiên này bằng khoá riêng của mình và nhận được khoá phiên. Khoá phiên này sẽ là khoá sử dụng để trao đổi dữ liệu giữa hai máy. Quá trình này được xem như các bước nhận diện máy chủ và máy khách. Kiểu mã hóa an toàn tập tin trên đường truyền này của SSH cũng giống với cơ chế của SSL (Giao thức https trên trình duyệt)

***Mã hoá dữ liệu***

Sau khi hoàn tất việc thiết lập phiên làm việc bảo mật (trao đổi khoá, định danh), quá trình trao đổi dữ liệu diễn ra thông qua một bước trung gian đó là mã hoá/giải mã. Điều đó có nghĩa là dữ liệu gửi/nhận trên đường truyền đều được mã hoá và giải mã theo cơ chế đã thoả thuận trước giữa máy chủ và máy khách. Việc lựa chọn cơ chế mã hoá thường do máy khách quyết định. Các cơ chế mã hoá thường được chọn bao gồm: 3DES, IDEA, và Blowfish. Khi cơ chế mã hoá được lựa chọn, máy chủ và máy khách trao đổi khoá mã hoá cho nhau. Việc trao đổi này cũng được bảo mật dựa trên đinh danh bí mật của các máy. Kẻ tấn công khó có thể đánh cắp và giải mã thông tin trao đổi trên đường truyền vì không biết được khoá mã hoá. Các thuật toán mã hoá khác nhau và các ưu, nhược điểm của từng loại:

3DES (cũng được biết như Triple-DES) -- phương pháp mã hoá mặc định cho SSH.  
IDEA—Nhanh hơn 3DES, nhưng chậm hơn Arcfour và Blowfish.  
Arcfour—Nhanh, nhưng các vấn đề bảo mật đã được phát hiện.  
Blowfish—Nhanh và bảo mật, nhưng các phương pháp mã hoá đang được cải tiến.

***Chứng thực và giải mã***

Việc chứng thực là bước cuối cùng trong ba bước, và là bước đa dạng nhất. Tại thời điểm này, kênh trao đổi bản thân nó đã được bảo mật. Mỗi định danh và truy nhập của người sử dụng có thể được cung cấp theo rất nhiều cách khác nhau. Chẳng hạn, kiểu chứng thực rhosts có thể được sử dụng, nhưng không phải là mặc định; nó đơn giản chỉ kiểm tra định danh của máy khách được liệt kê trong file rhost (theo DNS và địa chỉ IP). Việc chứng thực mật khẩu là một cách rất thông dụng để định danh người sử dụng, nhưng ngoài ra cũng có các cách khác: chứng thực RSA, sử dụng ssh-keygen và ssh-agent để chứng thực các cặp khoá.

SSH là một giao thức rất linh hoạt, và có rất nhiều cách (kiểu mã hóa) khác nhau. kiến trúc mở của giao thức cho phép các dịch vụ này để chạy cùng một lúc mà không cản trở nhau.

**SSH an toàn như thế nào?**

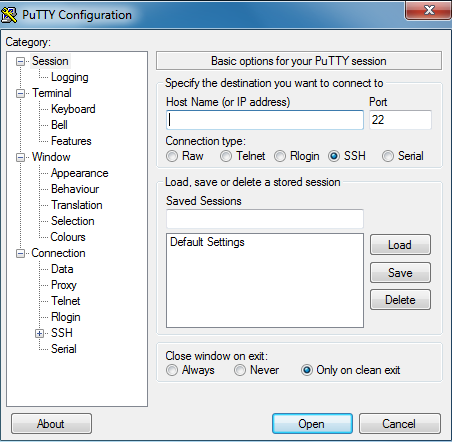
Các giao thức SSH phiên bản 2 cung cấp các dịch vụ của máy chủ: xác thực; mã hóa; xác minh tính toàn vẹn dữ liệu; và xác thực khách hàng. máy chủ xác thực được thực hiện bằng DSA, RSA hoặc ECDSA thuật toán mã khóa công khai. Để xác minh mã hóa và toàn vẹn dữ liệu, một số thuật toán được cung cấp mà mỗi sản phẩm SSH có thể thực hiện trong một khoảng thời gian nhất định. xác thực khách hàng có thể được thực hiện bằng cách sử dụng mật khẩu, khóa công khai, chỉ 1 tài khoản login trên 1 thời diểm (single sign-on), và các phương pháp khác.

Đặc điểm kỹ thuật giao thức [SSH2](https://hostingviet.vn/ssh-la-gi) được công khai và đã được xem xét bởi một số người thực hiện độc lập. Khi thực hiện đúng và sử dụng, các giao thức được cho là an toàn chống lại tất cả các cuộc tấn công mật mã được biết đến.

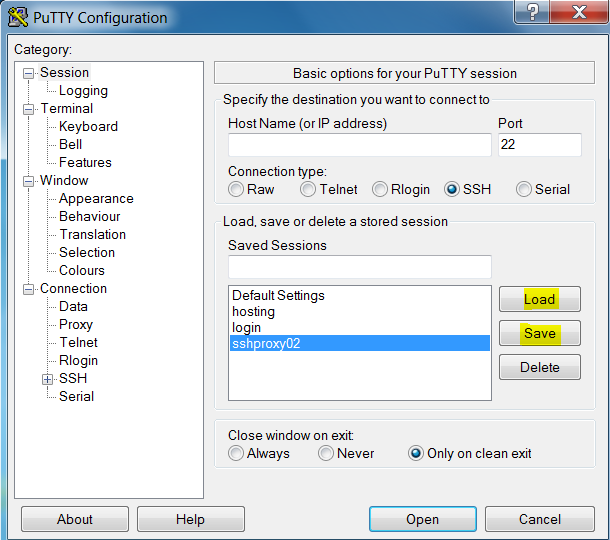
2. Hướng dẫn sử dụng phần mềm PuTTY để SSH vào VPS/Server Linux.

PuTTY là một phần mềm cho phép kết nối đến máy chủ (VPS/Server Linux) qua giao thức SSH để thực hiện các điều khiển bằng dòng lệnh (command line). Để sử dụng PuTTY khách hàng cần download phần mềm này về máy tính. Khách  hàng có thể tải từ trang chủ bản cài đặt hoặc bản dùng ngay.

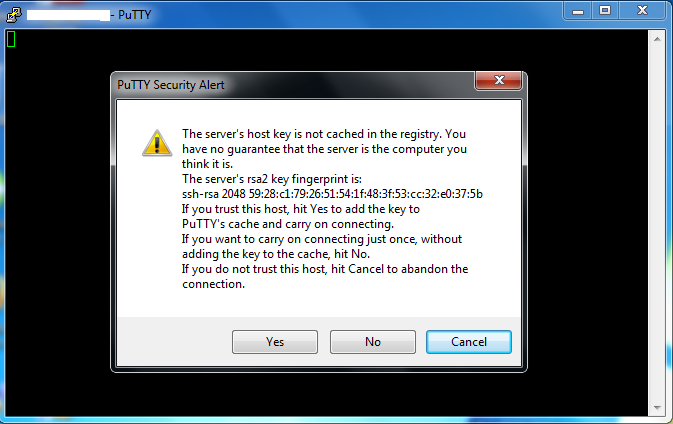
**2.1. Mở chương trình PuTTY vừa tải về/cài đặt.**



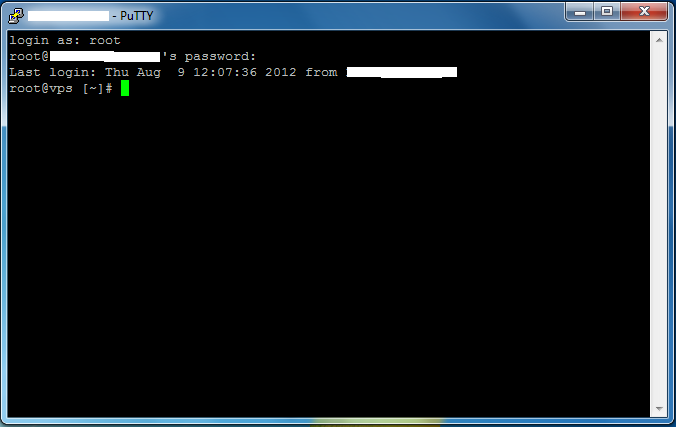
**2.2. Nhập thông tin Server cần điều khiển.**

    Hostname/IP Address: nhập vào IP hoặc Hostname của Server.  
  
    Port: mặc định là cổng 22.  
  
    Connection Type :  SSH  
  
   Ở mục Saved Session: khách hàng có thể lưu lại các kết nối để lần sau không phải nhập lại các thông tin. Điền tên session vào ô Saved   
    Session và chọn Save. Nếu đã lưu thành công thì khách hàng chỉ cần chọn vào tên session Sau đó chọn Load để tạo kết nối.  
      
  
  
   Cuối cùng chọn Open để kết nối.

**2.3. Hiện ra cửa sổ thông báo.**

   Ở lần kết nối đầu tiên khách hàng sẽ nhận được thông báo như bên dưới. Chọn Yes để tiếp tục.  
  
   

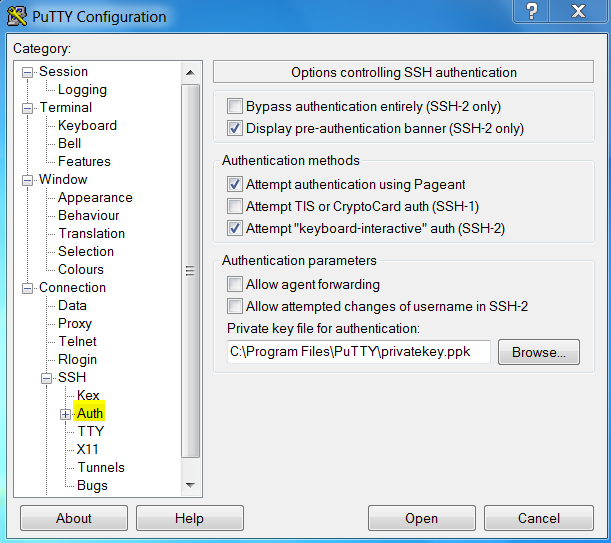
**2.4. Nhập thông tin username và password.**

   Nhập username và password để đăng nhập vào server. Lưu ý là dùng Enter sau mỗi lần nhập username/password. Password sẽ không được hiển thị ra khi nhập nên cần nhập chính xác rồi sau đó Enter.  
  
  
  
   Tại cửa sổ commandline khách hàng có thể sử dụng các lệnh để cấu hình cho server. Có thể tham khảo một số lệnh điều khiển dành cho Linux tại    đây.

**2.5. Một vài mẹo nhỏ sử dụng PuTTY.**

Bôi đen đoạn nào đó tức là copy nội dung của đoạn đó vào clipboard (tương đương với Ctrl + C)  
Chuột phải vào PuTTY tương đương với Paste nội dung đã được copy lên PuTTY (tương đương với Ctrl + V)

3. Hướng dẫn tạo kết nối dùng Private key

   Đối với các máy chủ sử dụng phương thức xác thực tài khoản bằng Private key. Sau khi đã nhập thông tin HostName (or IP Address) khách   
   hàng cần chọn mục Connection =>SSH => Auth bên phần Category. Sau đó chọn đến file Private key.  
     
  
   Sau đó chọn Open để tạo kết nối.

4. Cách cấu hình  cho dịch vụ SSH.

**4.1. Cấu hình chỉ cho shh bằng key**

     Việc truy cập ssh bằng mật khẩu rất nguy hiểm, nên đôi khi người quản trị chỉ muốn cho phép ssh bằng key. Để làm việc này cần  mở file    
     /etc/ssh/sshd\_config  hãy đảm bảo rằng có 2 dòng sau  
  
     PubKeyAuthentication yes  
  
     AuthorizedkeysFile .ssh/authorized\_keys  
  
     Sau đó tìm dòng:   
  
     PasswordAuthentication yes  
  
     Và đổi yes thành no.  
     Sau đó restart lại dịch vụ  /etc/init.d/ssh restart   
  
     Chú ý: nên để = yes, sau khi cấu hình SSH public key và private key thành công thì chuyển lại về thành = no

**4.2. Cấu hình chỉ cho phép một số người dùng được quyền ssh**

    Vì lí do bảo mật khách hàng có thể không cho user root có quyền ssh bằng cách mở file /etc/ssh/sshd\_config  tìm dòng sau và đổi yes thành no.  
  
    PermitRootLogin yes  
  
     Nếu muốn cho user bất kì nào đó có quyền ssh thì chỉ cần  thêm 1 dòng  
  
    AllowUsers user1 user2  
  
    Sau đó restart lại dịch vụ  /etc/init.d/ssh restart

**4.3. Cấu hình thay đổi port SSH**

    Mặc định SSH sử dụng cổng 22 để kết nối, các hacker có thể lợi dụng điều này để tấn công vào server. Vì thế khách hàng có thể bảo mật server  
    của mình hơn bằng cách thay đổi port ssh.  
  
    Mở file /etc/ssh/sshd\_config và tìm dòng có ghi:  
  
    Port 22  
  
    Thay đổi số cổng và khởi động lại dịch vụ SSH bằng lệnh:  
  
    /etc/init.d/ssh restart

**4.4. Cấu hình chỉ cho phép kết nối ssh từ một số host nhất định.**

    Danh sách các host bị cấm ssh được lưu trong file /etc/host.deny. Giả sử chúng ta có file /etc/host.deny có nội dung như sau:  
  
    sshd: ALL  
  
    và file /etc/host.allow  
  
    sshd: 192.168.1.2  
  
    thì chỉ có host 192.168.1.2 mới có quyền truy cập ssh còn các host còn lại sẽ bị cấm truy cập.  
  
    Ngoài ra khách hàng có thể tham khảo thêm một số các cấu hình cho dịch vụ ssh tại đây.

5.Jailed Shell SSH dành cho gói dịch vụ Hosting

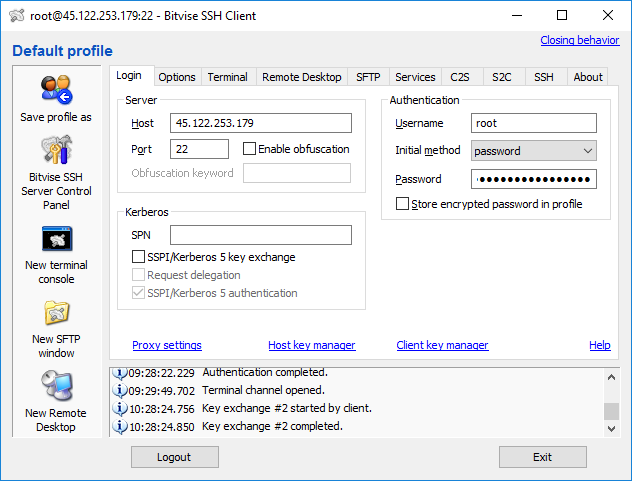
  
Đối với gói dịch vụ Hosting của Vinahost vẫn có hỗ trợ tính năng SSH cho khách hàng. Mặc định tính năng này sẽ bị đóng, để có thể sử dụng tính năng SSH, khách hàng liên hệ bộ phận kinh doanh để kích hoạt. Với tính năng này khách hàng có thể truy cập SSH thông qua tài khoản được cấp, được sử dụng các lệnh cơ bản của Linux, tuy nhiên vì SSH chạy chế độ "Jailed", nên sẽ bị giới hạn quyền quản lý và sử dụng.

# Bitvise SSH là gì? cách sử dụng phần mềm Bitvise SSH

Bitvise SSH là phần mềm miễn phí truy cập SSH. cài đặt và sử dụng trên nền tảng windows. Các nền tảng win được hỗ trợ bao gồm tất cả các máy tính để bàn và máy chủ, bắt đầu từ Windows XP và Windows Server 2003, đến gần đây nhất; bao gồm Windows 10 và Windows Server 2016. Cả hai 32-bit và 64-bit phiên bản của Windows được hỗ trợ. Bitvise SSH tương tự như phần mềm [PuTTY](https://hostingviet.vn/putty-la-gi-cach-su-dung-phan-mem-putty), OpenSSH

## ****Bitvise SSH là gì?****

Bitvise SSH là phần mềm miễn phí truy cập SSH. cài đặt và sử dụng trên nền tảng windows. Các nền tảng win được hỗ trợ bao gồm tất cả các máy tính để bàn và máy chủ, bắt đầu từ Windows XP và Windows Server 2003, đến gần đây nhất; bao gồm Windows 10 và Windows Server 2016. Cả hai 32-bit và 64-bit phiên bản của Windows được hỗ trợ. [**Bitvise SSH**](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh) tương tự như phần mềm [PuTTY](https://hostingviet.vn/putty-la-gi-cach-su-dung-phan-mem-putty), OpenSSH

[](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh)

Giao diện chính của bitvise ssh

## ****Đặc điểm nổi bật Bitvise ssh:****

**Dễ sử dụng:** Bitvise SSH Server đã được viết riêng cho nền tảng Windows vì vậy nó rất dễ dàng để cài đặt và cấu hình. Bạn có thể bật, tắt màn hình cmd, bật tắt bộ công cụ quản lý file (giống như filezilla). Đặc điểm này khiến mình thích thú với Bitvise SSH hơn là Putty.  
**Kết nối không giới hạn:** Bitvise SSH Server không áp đặt giới hạn về số lượng người dùng có thể kết nối đồng thời.  
**Tốc độ:** tốc độ truyền SFTP chủ yếu phụ thuộc vào kết nối giữa máy tính của khách hàng đến server, nhưng Bitvise SSH Server cho phép khách hàng có được một số của tốc độ truyền nhanh nhất hiện nay. Với Bitvise SSH Client, tốc độ truyền tập tin SFTP có thể lên đến hàng trăm MB/s.   
An toàn và đáng tin cậy: Cơ chế của Bitvise SSH đảm bảo an toàn dữ liệu.  
**Giới hạn băng thông:** upload riêng biệt và giới hạn tốc độ download có thể được cấu hình cho mỗi người dùng và nhóm.  
**Hỗ trợ thiết bị đầu cuối xuất sắc**: Bitvise SSH Server cung cấp sự hỗ trợ thiết bị đầu cuối tốt nhất hiện có trên nền tảng Windows. Và khi được sử dụng với Bitvise SSH Client, giao thức bvterm hỗ trợ đầy đủ tính năng Windows giao diện điều khiển của: màu sắc, ký tự Unicode, và bộ đệm cuộn lớn.  
**Tính linh hoạt:** hầu hết các tính năng máy chủ SSH có thể được cấu hình riêng trên một cơ sở cho mỗi tài khoản từ người sử dụng thân thiện Bitvise SSH Server Control Panel. Sử dụng Bitvise SSH Client, Control Panel SSH server có thể được truy cập và cấu hình thông qua giao diện người dùng thân thiện cùng một từ bất kỳ địa điểm từ xa.

\* Tham khảo dịch vụ: [**Hosting giá rẻ**](https://hostingviet.vn/hosting-gia-re)

## ****Cài đặt phần mềm Bitvise SSH****

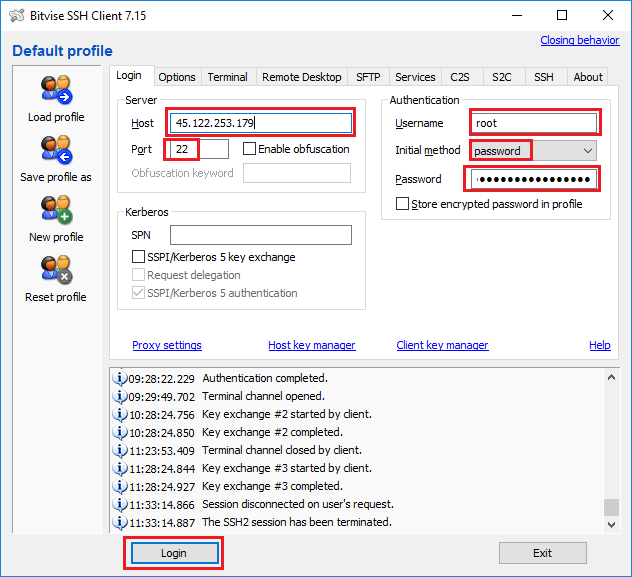
để cài đặt Bạn hãy Download [**Bitvise SSH Client**](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh) (Tunnelier) tại đây https://www.bitvise.com/ssh-client-download

Sau đó cài đặt như các phần mềm khác trên windows

## ****Đăng nhập và****[sử dụng Bitvise SSH Client](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh)

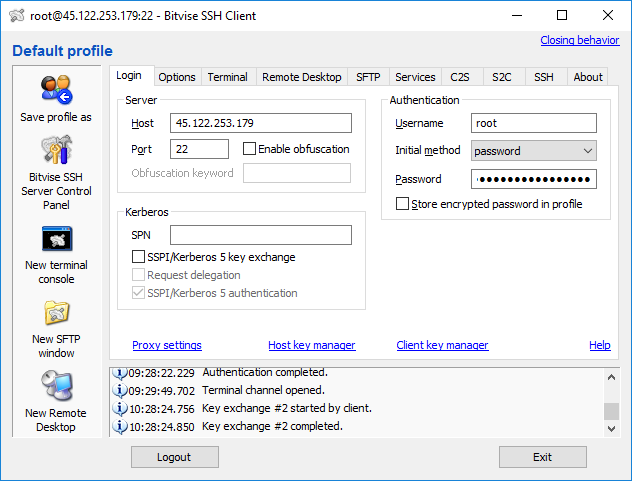
Để đăng nhập Bạn cần có đầy đủ thông tin truy cập SSH của server đã cài đặt hệ điều hành linux. Thường sử dụng centos nhé. Thông tin bao gồm: Địa chỉ IP, user name (thường là root), password và port (cổng - mặc định là 22).

***Bạn hãy nhập thông số như sau:***

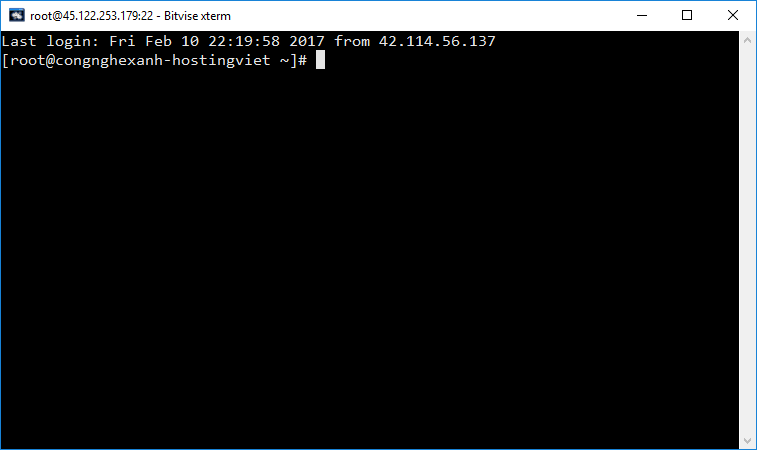
[](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh)

Nhập IP tại Host  
Nhập Port  
nhập username  
chọn kiểu bảo mật là password  
nhập password  
Click "Login"

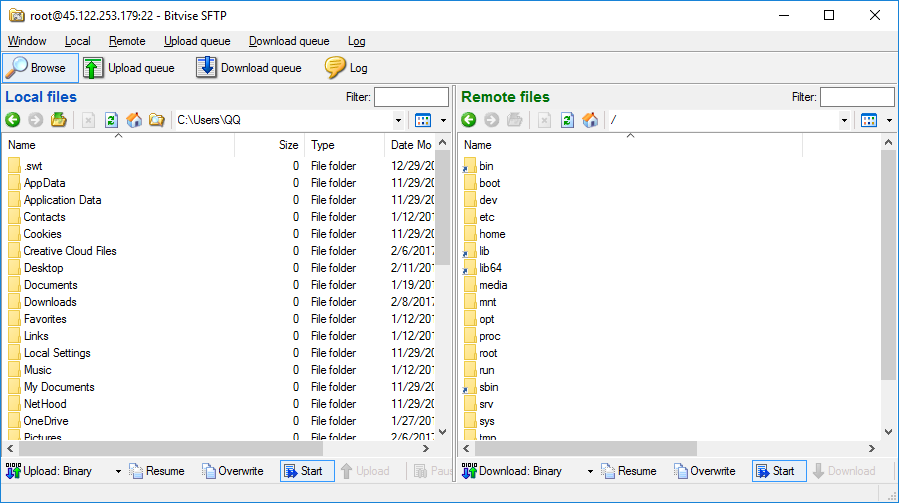
Nếu đăng nhập thành công thì giao diện sẽ như sau:

[](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh)

Sau khi đăng nhập thành công Bitvise SSH Client sẽ tự mở cửa sổ "Terminal console" nơi Bạn thực thi các lệnh với vps. Và cửa sổ SFTP (quản lý File).

[](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh)

Màn hình Console

[](https://hostingviet.vn/bitvise-ssh-la-gi-cach-su-dung-phan-mem-bitvise-ssh)

Màn hình SFTP