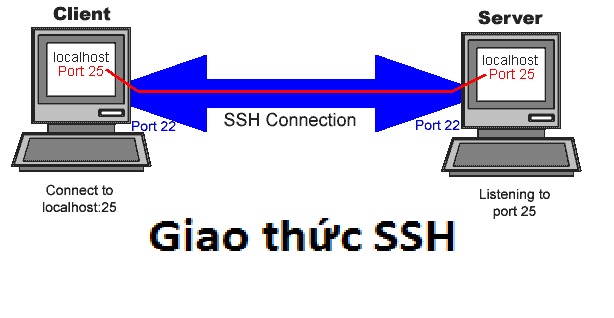
BÁO CÁO TÌM HIỂU VỀ SSH

1. **Khái niệm**

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.

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

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

1. Đặc điểm của SSH

* Tính bí mật (Privacy) do sử dụng các cơ chế mã hóa mạnh mẽ
* Tính toàn vẹn (Integrity) đảm bảo tính toàn vẹn dữ liệu trên đường truyền.
* Chứng minh xác thực (Authentication) sử dụng những phương pháp xác thực giữa Client và Server
* Giấy phép (Authorization) :dùng để điều khiển truy cập đến tài khoản.
* Chuyển tiếp (Forwarding) hoặc tạo đường hầm (tunneling) để mã hoá những phiên khác dựa trên giao thức TCP/IP

1. Cấu trúc của SSH

* Server

Một chương trình cho phép đi vào kết nối SSH với một bộ máy, trình bày xác thực, cấp phép, … Trong hầu hết SSH bổ sung của Unix thì server thường là sshd.

* Client

Một chương trình kết nối đến SSH server và đưa ra yêu cầu như là “log me in” hoặc “copy this file”. Trong SSH1, SSH2 và OpenSSH, client chủ yếu là ssh và scp.

* Session

Một phiên kết nối giữa một client và một server. Nó bắt đầu sau khi client xác thực thành công đến một server và kết thúc khi kết nối chấm dứt. Session có thể được tương tác với nhau hoặc có thể là một chuyến riêng.

* Key

Một lượng dữ liệu tương đối nhỏ, thông thường từ mười đến một hoặc hai ngàn bit. Tính hữu ích của việc sử dụng thuật toán ràng buộc khoá hoạt động trong vài cách để giữ khoá: trong mã hoá, nó chắc chắn rằng chỉ người nào đó giữ khoá (hoặc một ai có liên quan) có thể giải mã thông điệp, trong xác thực, nó cho phép bạn kiểm tra trễ rằng người giữ khoá thực sự đã kí hiệu vào thông điệp.

Có hai loại khóa: khoá đối xứng hoặc khoá bí mật và khoá bất đối xứng hoặc khóa công khai. Một khoá bất đối xứng hoặc khoá công khai có hai phần: thành phần công khai và thàn phần bí mật.

1. **Cách hoạt động của SSH**

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 hóa: thiết lập kênh làm việc mã hóa
* 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.

***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.

1. Một số thuật toán trong SSH

* Thuật toán Public-keys (Khóa công khai)

RSA: là thuật toán mã hóa bất đối xứng, dùng cho mã hóa và chữ ký

DSA: dùng chữ ký số

Thuật toán thỏa thuận Diffie-Hellman: cho phép 2 bên lấy được khóa được chia sẻ trên một kênh mở

* Thuật toán Private-keys (Khóa bí mật)

AES: là một thuật toán mã hóa khối, chiều dài có thể là 128 đến 256bit.

DES: là một thuật toán mã hóa bảo mật

3DES: cải tiến của DES, tăng độ dài của khóa để đạt độ bảo mật cao hơn

RC4: Kiểu mã hóa nhanh, nhưng kém bảo mật

Blowfish: là một thuật toán mã hóa miễn phí, có tốc độ mã hóa nhanh hơn DES, nhưng chậm hơn RC4. Độ dài của key từ 32 đến 448bit.

* Hàm băm (HASH)

CRS-32: Băm dữ liệu nhưng không mã hóa. Chỉ sử dụng để kiểm tra tính toàn vẹn của gói tin, tránh thay đổi thông tin trên đường truyền

MD5: Hàm băm có độ an toàn cao vì được mã hóa dữ liệu, với chiều dài là 128bit.

SHA-1: Một cải tiến của MD5, với chiều dài là 160bit.