

1. **Xây dựng kết nối TCP**: Máy khách SSH thiết lập kết nối mạng TCP với máy chủ SSH.

Mục đích :

* **Đảm bảo truyền dữ liệu đáng tin cậy**: TCP đảm bảo rằng tất cả các gói dữ liệu được gửi giữa hai máy tính sẽ đến đích mà không bị mất hoặc bị lặp lại. Nếu có gói bị mất, TCP sẽ tự động yêu cầu gửi lại.
* **Sắp xếp dữ liệu**: TCP đảm bảo rằng các gói dữ liệu được gửi theo đúng thứ tự, giúp việc xử lý dữ liệu trở nên dễ dàng hơn

2. **Chọn phiên bản hỗ trợ:** Chọn phiên bản hỗ trợ cho cả 2

**3.** **Thương lượng thuật toán hỗ trợ**: Cả hai bên thương lượng để chọn các thuật toán mã hóa, xác thực và nén mà cả hai đều có thể sử dụng.

4. **Tạo cặp khóa**: Máy khách tạo một cặp khóa bao gồm khóa công khai và khóa riêng tư.

**5. Gửi khóa công khai**: Máy khách gửi khóa công khai đến máy chủ.

**6. Khởi tạo yêu cầu đăng nhập**: Máy khách khởi tạo yêu cầu đăng nhập vào máy chủ.

**7. Máy chủ tìm thấy khóa phù hợp, mã hóa thông điệp bằng khóa công khai**: Máy chủ kiểm tra xem khóa công khai nhận được có tồn tại trong danh sách các khóa đã được ủy quyền (

~/.ssh/authorized\_keys

) hay không. Nếu có, nó sẽ sử dụng khóa công khai này để mã hóa một số ngẫu nhiên.

**8. Trả lại số ngẫu nhiên đã được mã hóa**: Máy chủ trả lại số ngẫu nhiên đã được mã hóa bằng khóa công khai đó đến máy khách.

**9. Giải mã dữ liệu bằng khóa riêng tư**: Máy khách sử dụng khóa riêng tư của mình để giải mã số ngẫu nhiên được gửi từ máy chủ.

**10. Gửi dữ liệu đã được giải mã**: Máy khách gửi số ngẫu nhiên đã được giải mã trở lại cho máy chủ.

**11. Máy chủ xác nhận việc giải mã là đúng**: Máy chủ kiểm tra số ngẫu nhiên đã được giải mã để đảm bảo rằng máy khách có quyền truy cập.

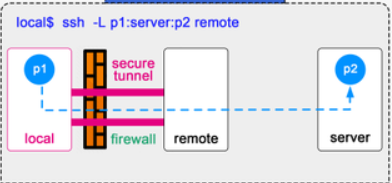
**12. Yêu cầu và phản hồi phiên làm việc**: Cả hai bên tiếp tục quy trình yêu cầu và phản hồi để thiết lập một phiên làm việc an toàn.

**13. Gửi lệnh đã được mã hóa**: Máy khách gửi các lệnh đã được mã hóa đến máy chủ.

**14. Giải mã lệnh bằng khóa phiên làm việc**: Máy chủ sử dụng khóa phiên làm việc để giải mã lệnh.

**15. Gửi kết quả đã được mã hóa**: Máy chủ thực hiện lệnh và gửi kết quả đã được mã hóa trở lại cho máy khách.

**16. Giải mã kết quả bằng khóa phiên làm việc**: Máy khách sử dụng khóa phiên làm việc để giải mã kết quả.



1. **SSH Local Forwarding**:

* Đây là quá trình chuyển tiếp cổng địa phương.
* Lệnh

ssh -L p1:server:p2 remote

 được sử dụng để tạo một đường hầm SSH từ cổng địa phương

p1

 đến cổng

p2

 trên máy chủ xa

server

.

* Điều này giúp người dùng có thể truy cập vào dịch vụ đang chạy trên cổng

p2

 của máy chủ từ cổng

p1

 trên máy khách. Qua đó, SSH không chỉ cung cấp khả năng truyền dữ liệu an toàn mà còn cho phép chuyển tiếp cổng để truy cập vào các dịch vụ khác nhau qua tường lửa hoặc các rào cản mạng khác.