# **BÀI 3: TRIỂN KHAI GIAO THỨC SSH**

## 3.1. Mô Hình

A close-up of a magnifying glass

Description automatically generated

* Mô hình triển khai giống như mô hình triển khai giao thức IPsec

## 3.2. Triển khai giao thức

* Cài đặt gói phần mềm openssh-server trên cả hai máy Client và Server

A black background with white text

Description automatically generated

A black background with white text

Description automatically generated

* Cấu hình file /etc/ssh/sshd\_config trên cả 2 máy Client và Server

A close up of words

Description automatically generated

* Bỏ dấu thăng ở đầu dòng PasswordAuthentication yes
* Khởi động lại dịch vụ ssh và kiểm tra trạng thái dích vụ ssh sau khi cấu hình

A computer screen shot of a program

Description automatically generated

A computer screen shot of a program

Description automatically generated

* Ta thấy trạng thái đã active
* Ta tiến hành kết nối đến máy chủ Server

A screenshot of a computer

Description automatically generated

* Kết nối đến máy chủ thành công
* Các gói tin bắt được

A screenshot of a computer

Description automatically generated

* Nội dung gói tin đã bị mã hoá

A group of white lines with different colored spots

Description automatically generated with medium confidence

A screen shot of a computer

Description automatically generated

* Encryption: chacha20-poly1305@openssh.com : Đây là thuật toán mã hóa ChaCha20-Poly1305, một phương pháp mã hóa hiện đại, hiệu suất cao và an toàn do OpenSSH cung cấp
* MAC: <implicit>: Cơ chế kiểm tra tính toàn vẹn của dữ liệu (Message Authentication Code) được thực hiện ẩn (implicit)
* Compression: none Dữ liệu không được nén trong phiên SSH này.
* Packet Length: 1532 là tổng độ dài gói tin SSH trong quá trình truyền dữ liệu
* Padding Length: 7 là độ dài của dữ liệu đệm (padding) để đảm bảo kích thước gói phù hợp với giao thức SSH
* **Method:** [sntrup761x25519-sha512@openssh.com](mailto:sntrup761x25519-sha512@openssh.com) là phương pháp trao đổi khóa kết hợp giữa hai thuật toán sntrup761 và x25519. SHA-512 là hàm băm trong quá trình tạo khoá
* Message Code: Key Exchange Init (20) với mã tin nhắn là 20 chỉ ra đây là gói tin khởi tạo trao đổi khoá
* Sequence Number: 0 là số thứ tự của gói tin trong quá trình trao đổi dữ liệu giữa Client và Server
* Dùng lệnh ssh-keygen để tạo khoá bí mật và công khai

A computer screen shot of a computer code

Description automatically generated

* Khoá bí mật sẽ được lưu trong file /root/.ssh/id\_ed25519
* Khoá công khai sẽ được lưu trong file /root/.ssh/id\_ed25519.pub
* Key fingerprint: khoá công khai đã được băm bằng SHA-256
* root@client: tên người dùng và máy đã tạo khoá
* Xem khoá bí mật

A computer code with white letters and numbers

Description automatically generated

* Xem khoá công khai



* Sao chép khoá công khai vào máy Server

A computer code on a black background

Description automatically generated

* Number of key(s) added: 1 số lượng khoá sao chép là 1
* Kết nối với Server mà không cần phải mật khẩu vì đã có khoá công khai

A computer screen shot of a computer

Description automatically generated

A computer screen shot of a number

Description automatically generated

* Encrypted Packet: nội dung của gói tin đã được mã hóa
* [Direction: client-to-server]: gói tin từ Client gửi đến Server

## 3.3. Tổng kết

* Triển khai được giao thức SSH, sinh khoá ngẫu nhiên cho server từ bên ngoài và triển khai xác thực người dùng từ mã công khai
* SSH là giao thức kết nối bảo mật hơn Telnet và vì vậy hiện nay giao thức SSH được sử dụng phổ biến hơn