# **BÀI 1: TRIỂN KHAI GIAO THỨC IPSEC**

## 1.1. Mô hình

A long black and silver bar with a blue circle

Description automatically generated

* Chỉnh lại card mạng cho 2 máy: Hai máy dùng VMnet2

A screenshot of a computer

Description automatically generated

* Thêm card mạng NAT cho 2 máy để cài đặt gói qua internet, nằm ngoài mô hình đã thiết kế

A screenshot of a computer

Description automatically generated

* Set IP cho máy Client

A screenshot of a computer

Description automatically generated

* Set IP cho máy Server

A screenshot of a computer

Description automatically generated

## 1.2. Triển khai giao thức

* Cài đặt strongswan cho 2 máy Client và Server

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer program

Description automatically generated

* Set host name cho Client và Server và sửa đổi file hosts

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

* Đặt 10.5.14.5 với hostname là server
* Đặt 10.5.14.105 với hostname là client
* Sau khi set hostname thì ta có thể thực hiện ping + hostname thay vị địa chỉ IP

A screenshot of a computer program

Description automatically generated

A computer screen shot of a program

Description automatically generated

* Sau khi cài công cụ Strongswan thì trong /etc sẽ có 3 file như hình dưới

A screenshot of a computer screen

Description automatically generated

* Cấu hình file ipsec.secrets trên 2 máy Client và Server để chia sẻ khoá



A screenshot of a computer

Description automatically generated

A computer screen with text and numbers

Description automatically generated

* Địa chỉ của máy nào là máy chủ của khoá thì sẽ viết IP trước
* PSK: Pre-Share Key là một **khóa được chia sẻ trước** giữa hai hoặc nhiều thực thể để xác thực và mã hóa dữ liệu trong một giao thức bảo mật
* Hai PSK này phải giống nhau

### 1.2.1. Triển khai AH Transport

* Cấu hình file ipsec.conf trên Server và Client



A computer screen shot of a code

Description automatically generated

A screenshot of a computer program

Description automatically generated

* conn transportAH: Định nghĩa một kết nối IPsec có tên transportAH
* type=transport: Chế độ Transport Mode
* left: Địa chỉ IP của máy chủ hiện tại
* right: Địa chỉ IP của máy đối tác
* authby=secret: Xác thực bằng Pre-Shared Key (PSK)
* ah=aes128-sha1: Dùng AH (Authentication Header) với thuật toán xác thực AES-128 và SHA-1 để kiểm tra tính toàn vẹn
* auto=start: Tự động khởi động kết nối IPsec khi dịch vụ IPsec chạy
* Khởi động lại giao thức ipsec trên 2 máy Client và Server

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* Kiểm tra trạng thái của giao thức

A computer code with numbers and letters

Description automatically generated

* Security Associations (1 up, 0 connecting):
* Có 1 kết nối đang hoạt động (up), không có kết nối nào đang chờ thiết lập (0 connecting)
* Điều này cho thấy IPsec đã thiết lập thành công giữa hai máy
* ESTABLISHED 20 seconds ago: Kết nối transportAH đã được thiết lập 20 giây trước.
* transportAH{1}: INSTALLED, TRANSPORT, reqid 1, AH SPIs: c4d64a03\_i c6386503\_o
* Kết nối đã được cài đặt (INSTALLED) và sử dụng TRANSPORT mode
* reqid 1: Request ID yêu cầu để xác định chính sách IPsec (Policy ID)
* AH SPIs (Security Parameter Index): là một giá trị 32-bit giúp nhận diện Security Association (SA) trong giao thức IPsec Authentication Header (AH).
* Thực hiện ping 2 máy và bắt gói tin

A screenshot of a computer

Description automatically generated

* Các gói tin bắt được trong quá trình ping
* Gói tin có AH (Authentication Header)

A screenshot of a computer

Description automatically generated

* protocol: Authentication Header (51) với 51 là mã giao thức của AH
* Next Header: ICMP(1) xác định gói tin tiếp theo là ICMP với mã là 1
* Length: Độ dài của Authentication Header
* Reverved: Trường dự trữ
* AH SPI: là một giá trị 32-bit giúp nhận diện Security Association (SA) trong giao thức IPsec Authentication Header (AH).
* AH Sequence: Số thứ tự của gói tin
* AH ICV (Integrity Check Value): Giá trị xác thực (hash) dùng để kiểm tra tính toàn vẹn
* ICV = hash(IP Header + Payload + Key)
* Gói tin không trong chế độ Transport AH nên không có AH

A screen shot of a computer

Description automatically generated

### 1.2.2. Triển khai ESP Transport

* Cấu hình file ipsec.conf trên 2 máy Client và Server

A screen shot of a computer code

Description automatically generated

A screenshot of a computer code

Description automatically generated

* conn transportESP: Định nghĩa một kết nối IPsec có tên transportESP
* esp=aes128-sha1: Cấu hình ESP với mã hóa AES-128 và xác thực SHA-1
* Khởi động lại giao thức ipsec trên 2 máy Client và Server

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* Kiểm tra trạng thái của giao thức

A screenshot of a computer

Description automatically generated

A computer screen shot of numbers

Description automatically generated

* Thực hiện ping 2 máy và bắt gói tin

A screenshot of a computer

Description automatically generated

* Các gói tin bắt được trong quá trình ping
* Gói tin ESP

A screenshot of a computer

Description automatically generated

* Protocol: Encap Security Payload (50) với 50 là mã của giao thức ESP
* ESP SPI là một giá trị 32-bit giúp nhận diện Security Association (SA) trong giao thức IPsec ESP.

### 1.2.3. Triển khai AH Tunnel

* Cấu hình file ipsec.conf trên 2 máy Client và Server

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

* conn tunnelAH: Định nghĩa một kết nối IPsec có tên tunnelAH
* ah=aes128-sha1: Cấu hình AH với mã hóa AES-128 và xác thực SHA-1
* Khởi động lại giao thức ipsec trên 2 máy Client và Server

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* Kiểm tra trạng thái của giao thức

A computer screen with numbers and letters

Description automatically generated

A computer screen shot of numbers

Description automatically generated

* Thực hiện ping 2 máy và bắt gói tin

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Next Header: IPIP (4) Giao thức tiếp theo là IPIP (IP-in-IP encapsulation) với mã là 4 => Chế độ Tunnel

### 1.2.4. Triển khai ESP Tunnel

* Cấu hình file ipsec.conf trên 2 máy Client và Server

A screenshot of a computer program

Description automatically generated

A screenshot of a computer code

Description automatically generated

* conn tunnelESP: Định nghĩa một kết nối IPsec có tên tunnelESP
* esp=aes128-sha1: Cấu hình ESP với mã hóa AES-128 và xác thực SHA-1
* Khởi động lại giao thức ipsec trên 2 máy Client và Server

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* Kiểm tra trạng thái của giao thức

A computer screen with numbers and letters

Description automatically generated

A computer screen with numbers and letters

Description automatically generated

* Thực hiện ping 2 máy và bắt gói tin

A screenshot of a computer

Description automatically generated

## 1.3. Tổng kết

* Authentication Header (AH)

- AH cung cấp dịch vụ đảm bảo toàn vẹn cho tất cả các header và data gói tin. Ngoại trừ một số trường IP Header mà định tuyến thay đổi trong chuyển tiếp.  
- AH bao gồm địa chỉ nguồn và địa chỉ đích trong dịch vụ đảm bảo toàn vẹn. AH thường không tương thích với NAT.  
- Hiện nay, hầu hết IPSec bổ sung hỗ trợ phiên bản thứ hai của IPSec mà ESP có thể cung cấp dịch các vụ đảm bảo toàn vẹn dữ liệu qua sự xác thực.  
- AH cung cấp một lợi ích mà ESP không có, đó là: đảm bảo toàn vẹn cho outermost IP Header

* Encapsulaton Secutity Payload (ESP)

- Trong Tunnel Mode, ESP cung cấp sự mã hoá và sự đảm bảo an toàn cho đóng gói IP Packet, cũng xác thực tốt giống như của ESP Header, ESP có thể tương thích với NAT.  
- Trong Transport Mode, ESP cung cấp sự mã hoá và đảm bảo an toàn cho Payload của gói tin IP, cũng đảm bảo an toàn tốt giống như của ESP Header. Transport Mode thì không tương thích với NAT.  
- ESP Tunnel Mode thường sử dụng phổ biến trong IPSec, vì nó mã hoá IP Header gốc, nó có thể giấu địa chỉ source và des thật của gói tin. ESP cũng có thể thêm vật đệm vào để đủ gói tin.  
- ESP thường được dùng để cung cấp cho mã hoá hoặc đảm bảo an toàn (hoặc cả hai).