TRƯỜNG ĐẠI HỌC KHOA HỌC HUẾ

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO TIỂU LUẬN

HỌC PHẦN: AN NINH MẠNG

ĐỀ TÀI: TÌM HIỂU VÀ TRIỂN KHAI IPSec VPN VỚI PHẦN MỀM GIẢ LẬP GNS3

Giảng viên hướng dẫn : Võ Việt Dũng

Sinh viên thực hiện : Đoàn Phạm Minh Quang

Hắc Thị Thu Hồng

Trần Đức Thăng

Phạm Bá Nhật Quang

Nguyễn Quốc Bảo

BẢNG PHÂN CÔNG NHIỆM VỤ

Stt	Họ & tên	Nhiệm vụ được phân công
1	Đoàn Phạm Minh Quang	- Tổng hợp tài liệu tham khảo về IPSec và VPN - Thực hiện Chương 1: Tổng quan về IPSec (khái niệm, lịch sử, ứng dụng) - Hỗ trợ chỉnh sửa nội dung lý thuyết
2	Hắc Thị Thu Hồng	- Nghiên cứu cấu trúc, thành phần và cơ chế bảo mật của IPSec - Thực hiện mục 1.2, 1.3 và 1.4 trong Chương 1 - Đóng góp nội dung ưu điểm, hạn chế
3	Trần Đức Thăng	- Nghiên cứu VPN và các mô hình triển khai - Thực hiện Chương 2: Tổng quan VPN (Remote Access, Site-to-Site, Intranet, Extranet) - Phân tích lợi ích và thách thức của VPN
4	Phạm Bá Nhật Quang	- Thực hiện mô hình IPSec VPN Site-to-Site trên GNS3 - Thiết kế sơ đồ mạng, cấu hình Router A & Router B - Kiểm tra kết nối và xác minh trạng thái IPSec
5	Nguyễn Quốc Bảo	- Thực hiện mô hình IPSec VPN Client-to-Site trên GNS3 - Cấu hình Router, VPN Client và kiểm tra kết nối - Tổng hợp kết quả thực nghiệm, viết Kết luận - Hoàn thiện báo cáo và quản lý nộp bài

MỤC LỤC

LỜI MỞ ĐẦU

Trong bối cảnh công nghệ thông tin ngày càng phát triển, việc bảo mật dữ liệu và đảm bảo kết nối an toàn trở nên vô cùng quan trọng. Mạng riêng ảo (VPN) đã trở thành một giải pháp thiết yếu cho các cá nhân và tổ chức muốn bảo vệ thông tin liên lạc của mình khỏi các nguy cơ tiềm ẩn trên mạng internet. Đặc biệt, giao thức IPSec được biết đến với khả năng bảo mật mạnh mẽ và tính linh hoạt cao. Bài tiểu luận này sẽ tập trung vào việc tìm hiểu về IPSec VPN và cách triển khai nó trong môi trường giả lập GNS3, một công cụ mạnh mẽ cho phép xây dựng và thử nghiệm các mô hình mạng phức tạp.

Chúng em xin chân thành cảm ơn sự giúp đỡ của thầy trong việc đưa ra những ý kiến cần thiết để làm nền tảng cho đề tài trên, chỉ dẫn trong việc sửa chữa các vấn đề bị sai sót hoặc thiếu đi phần quan trọng,....

Tuy nhiên trong quá trình thực hiện đề tài, vẫn không thể tránh khỏi những lỗi sai sót nhỏ, chúng em rất mong được nhận sự góp ý và đánh giá, cũng như lời khuyên của thầy để tránh lặp lại lỗi sai trong tương lai sau này.

CHƯƠNG 1: Tìm hiểu về hoạt động của giao thức IPSec

1.1. Giới thiệu về IPSec

1.1.1. Khái niệm

IPSec (Internet Protocol Security) là một bộ giao thức bảo mật mạnh mẽ cung cấp các công cụ để mã hóa, xác thực, và đảm bảo tính toàn vẹn của dữ liệu trong khi truyền qua mạng. Đây là một trong những giao thức quan trọng nhất trong bảo mật mạng.

1.1.2. Lịch sử phát triển

- IPSec được phát triển như một chuẩn bảo mật Internet do IETF (Internet Engineering Task Force) đề xuất.
- Nó xuất hiện như một giải pháp để bảo vệ tính bí mật và toàn vẹn của thông tin trong kỷ nguyên IPv4 và IPv6.

1.1.3. Ứng dụng thực tiễn

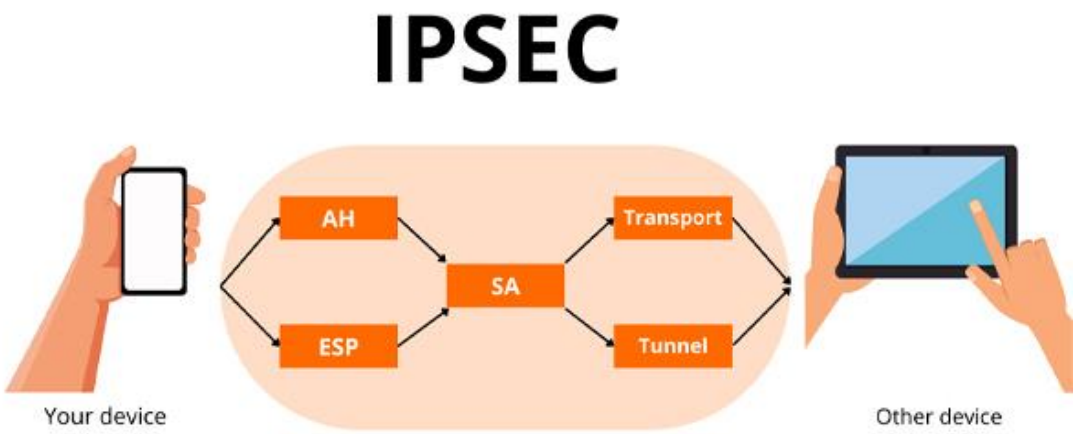
- Được sử dụng phổ biến trong môi trường VPN (Virtual Private Network) để thiết lập các kênh truyền dữ liệu an toàn.

- Bảo vệ hệ thống mạng doanh nghiệp, chống tấn công MITM (Man-in-the-Middle).

1.2. Cấu trúc và thành phần của IPSec

1.2.1. Kiến trúc tổng quát

IPSec là một bộ giao thức hoạt động tại tầng Internet (Network Layer) trong mô hình OSI, cung cấp bảo mật cho dữ liệu IP đang truyền.



1.2.2. Các thành phần chính

+ AH (Authentication Header):
  - Xác minh danh tính nguồn gốc dữ liệu.
  - Đảm bảo tính toàn vẹn của gói tin, nhưng không cung cấp tính bí mật.
+ ESP (Encapsulating Security Payload):
  - Mã hóa dữ liệu để bảo vệ tính bí mật.
  - Tích hợp tính năng xác thực và đảm bảo toàn vẹn.
+ IKE (Internet Key Exchange):
  - Giao thức trao đổi và quản lý khóa mã hóa.
  - Có 2 giai đoạn: thiết lập kênh bảo mật và trao đổi tham số bảo mật.

1.2.3. Chế độ hoạt động

+ Chế độ Transport Mode:
  - Bảo mật phần payload (dữ liệu).
  - Thích hợp trong giao tiếp nội bộn.
+ Chế độ Tunnel Mode:
  - Bảo mật toàn bộ gói tin.
  - Thường được sử dụng trong môi trường VPN.

1.3. Nguyên tắc hoạt động của IPSec

1.3.1. Quy trình thiết lập kết nối

- Giai đoạn 1: Thiết lập kênh bảo mật (Security Association - SA)

+ Security Association (SA): Là một tập hợp thông số dùng để thiết lập kết nối an toàn giữa các thiết bị.

+ Các bước thực hiện:

1. **Xác thực giữa hai bên:** Thiết bị xác minh danh tính của nhau, sử dụng mật mã đối xứng/asymmetric hoặc chứng chỉ số.

2. **Thương lượng thuật toán bảo mật:** Bao gồm thuật toán mã hóa, xác thực (như AES, SHA-256, v.v.).

3. **Chia sẻ khóa mã hóa:** Dựa vào thuật toán trao đổi khóa như Diffie-Hellman để tạo và trao đổi khóa bảo mật một cách an toàn.

4. **Tạo kênh bảo mật đầu tiên:** Còn được gọi là "IKE SA" (Internet Key Exchange SA), cho phép truyền dữ liệu trao đổi tham số bảo mật trong giai đoạn sau.

- Giai đoạn 2: Thảo luận và xác định tham số bảo mật

+ Thiết lập SA thứ hai: Gọi là "IPSec SA," được dùng để bảo vệ luồng dữ liệu thực sự.

+ Các bước chính:

1. Thương lượng tham số mã hóa và xác thực cuối cùng.

2. Xác định phạm vi bảo vệ (địa chỉ IP nguồn, đích, cổng, giao thức, v.v.).

3. Thiết lập cơ chế bảo vệ dữ liệu bằng giao thức ESP hoặc AH.

1.3.2. Cơ chế bảo mật

IPSec áp dụng các cơ chế bảo mật để bảo vệ dữ liệu khi truyền qua mạng:

1. Mã hóa dữ liệu:

- Bảo vệ tính bí mật của dữ liệu bằng cách mã hóa gói tin.
- **Giao thức ESP** thực hiện việc mã hóa thông tin quan trọng trong gói tin.
- Thuật toán phổ biến: **AES (Advanced Encryption Standard)**, DES, 3DES.

2. Xác thực:

- Đảm bảo rằng gói tin được gửi từ nguồn hợp lệ, chống lại các tấn công giả mạo.
- **Giao thức AH hoặc ESP** sử dụng các thuật toán băm (hash) như **HMAC-SHA256** hoặc **HMAC-MD5** để xác thực gói tin.

3. Toàn vẹn:

- Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền.
- Sử dụng mã xác thực thông điệp (Message Authentication Code - MAC) để phát hiện thay đổi.

1.3.3. Quản lý khóa

Quản lý khóa là thành phần quan trọng trong bảo mật IPSec, bao gồm:

1. Tạo khóa:

- Sử dụng các thuật toán trao đổi khóa như **Diffie-Hellman (DH)**.
- Diffie-Hellman hỗ trợ tạo ra các khóa chung giữa hai bên mà không cần truyền khóa rõ ràng qua mạng.

2. Trao đổi khóa:

- Thực hiện trong giai đoạn thiết lập IKE.
- Sử dụng kênh bảo mật IKE SA đã thiết lập để chia sẻ khóa, đảm bảo rằng khóa không bị đánh cắp hoặc sửa đổi trong quá trình trao đổi.

1.4. Ưu điểm và hạn chế của IPSec

1.4.1. Ưu điểm

- Tính bảo mật cao, đáp ứng nhiều yêu cầu nghiêm ngặt.
- Tính linh hoạt, có thể đối với nhiều giao thức mạng.

1.4.2. Hạn chế

- Cài đặt và cấu hình phức tạp.
- Tác động đến hiệu suất mạng do mã hóa và xác thực

CHƯƠNG 2: Tìm hiểu về VPN khái niệm & các mô hình triển khai

2.1. Khái niệm về VPN

VPN (Virtual Private Network) là một công nghệ mạng cho phép tạo ra kết nối an toàn và bảo mật qua một mạng công cộng như Internet. VPN được sử dụng để:

- Bảo vệ dữ liệu khi truyền tải qua mạng.
- Ẩn danh và che giấu địa chỉ IP của người dùng.
- Truy cập từ xa vào mạng nội bộ của tổ chức.
- Vượt qua các hạn chế về địa lý và kiểm duyệt internet.

+ Nguyên lý hoạt động:
  - VPN thiết lập một đường hầm (tunnel) giữa thiết bị người dùng và máy chủ VPN.
  - Dữ liệu được mã hóa trước khi truyền tải, giúp bảo vệ thông tin khỏi sự xâm nhập hoặc đánh cắp.

2.2. Các thành phần chính của VPN

1. Thiết bị khách (Client Device):
   - Máy tính, điện thoại hoặc các thiết bị khác có phần mềm VPN để kết nối.
2. Máy chủ VPN (VPN Server):
   - Máy chủ cung cấp dịch vụ VPN và xử lý yêu cầu kết nối.
3. Giao thức VPN:
   + Định nghĩa cách dữ liệu được mã hóa và truyền tải qua đường hầm. Các giao thức phổ biến:
   - PPTP (Point-to-Point Tunneling Protocol).
   - L2TP/IPSec (Layer 2 Tunneling Protocol).
   - OpenVPN.
   - IKEv2 (Internet Key Exchange v2).
4. Đường hầm VPN (VPN Tunnel):
   - Là kênh truyền dữ liệu mã hóa giữa thiết bị và máy chủ.

2.3. Lợi ích của VPN

- Bảo mật dữ liệu: Mã hóa dữ liệu và bảo vệ thông tin nhạy cảm.
- Tăng quyền riêng tư: Ẩn địa chỉ IP, tránh theo dõi trực tuyến.
- Truy cập từ xa: Nhân viên có thể kết nối vào hệ thống nội bộ dù ở xa.
- Vượt qua hạn chế địa lý: Truy cập nội dung bị giới hạn ở các khu vực khác nhau.

2.4. Các mô hình triển khai VPN

VPN được triển khai theo nhiều mô hình khác nhau tùy thuộc vào mục đích sử dụng:

2.4.1. VPN từ xa (Remote Access VPN)

+ Đặc điểm:
  - Kết nối người dùng từ xa vào mạng nội bộ của tổ chức.
  - Dữ liệu được mã hóa và truyền tải qua Internet.
+ Ứng dụng:
  - Nhân viên làm việc từ xa truy cập tài liệu công ty.
+ Ưu điểm:
  - Dễ triển khai, chi phí thấp.
  - Bảo mật cao nhờ mã hóa dữ liệu.
+ Nhược điểm:
  - Phụ thuộc vào tốc độ kết nối Internet.

2.4.2. VPN site-to-site

+ Đặc điểm:
  - Kết nối các mạng nội bộ của nhiều văn phòng, chi nhánh khác nhau.
  - Tạo thành một mạng lớn hoạt động thống nhất.
+ Ứng dụng:
  - Tổ chức lớn có nhiều chi nhánh cần trao đổi dữ liệu.
+ Ưu điểm:
  - Hoạt động ổn định, giảm chi phí thuê đường truyền riêng.
+ Nhược điểm:
  - Cần thiết bị chuyên dụng, thiết lập phức tạp hơn.

2.4.3. VPN Intranet và Extranet

1. Intranet VPN:
    - Kết nối giữa các văn phòng nội bộ của cùng một tổ chức.
    - Bảo mật và dễ quản lý.
2. Extranet VPN:
    - Kết nối giữa tổ chức với đối tác, khách hàng.
    - Bảo mật giao tiếp trong khi vẫn duy trì sự tách biệt.

2.5. Các thách thức và hạn chế của VPN

+ Hiệu suất:
    - Tốc độ truyền dữ liệu có thể giảm do mã hóa và giải mã.
+ Độ tin cậy:
    - Chất lượng kết nối phụ thuộc vào đường truyền Internet.
+ Quản lý:
    - Yêu cầu kỹ thuật cao để thiết lập và duy trì.
+ Chi phí:
    - Các tổ chức lớn cần đầu tư thiết bị và phần mềm chuyên dụng.

2.6. Tương lai của VPN

+ VPN và bảo mật mạng:
    - Tiếp tục đóng vai trò quan trọng trong việc bảo vệ dữ liệu cá nhân và doanh nghiệp.
+ Sự thay thế bởi các công nghệ mới:
    - Xuất hiện các công nghệ như ZTNA (Zero Trust Network Access), có thể thay thế một phần vai trò của VPN.
+ Ứng dụng AI và tự động hóa:
    - Giúp cải thiện hiệu suất và tăng khả năng phát hiện các mối đe dọa.

CHƯƠNG 3: Triển khai thử nghiệm IPSec trên GNS3

3.1. thử nghiệm theo mô hình site to site

1. Sơ đồ mạng

- **Router A**:
  - LAN: `192.168.1.0/24`
  - WAN: `10.1.1.1/30`
- **Router B**:
  - LAN: `192.168.2.0/24`
  - WAN: `10.1.1.2/30`
- **Mục tiêu**: Kết nối hai mạng LAN thông qua IPSec VPN.

2. Chuẩn bị trong GNS3

1. **Thêm các thiết bị**:
   - Hai router (Cisco IOS hoặc các thiết bị hỗ trợ IPSec).
   - Hai máy PC giả lập trong LAN của mỗi router.
2. **Kết nối thiết bị**:
   - Router A -> Internet Cloud (WAN).
   - Router B -> Internet Cloud (WAN).
   - Các PC kết nối LAN của từng router

3. Cấu hình Router A

Bước 1: Cấu hình IP cho các giao diện

```
interface gig0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown

interface gig0/1
 ip address 10.1.1.1 255.255.255.252
 no shutdown
```

Bước 2: Định tuyến tĩnh

```
ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

Bước 3: Cấu hình ISAKMP

```
crypto isakmp policy 10
 encryption aes
 hash sha256
 authentication pre-share
 group 2
crypto isakmp key vpn123 address 10.1.1.2
```

Bước 4: Tạo IPSec Transform Set

```
crypto ipsec transform-set VPN-TRANSFORM esp-aes esp-sha256-hmac
 mode tunnel
```

Bước 5: Tạo Crypto Map

```
 crypto map VPN-MAP 10 ipsec-isakmp
  set peer 10.1.1.2
  set transform-set VPN-TRANSFORM
  match address 101
```

Bước 6: Áp dụng Crypto Map vào Giao Diện WAN

```
interface gig0/1
 crypto map VPN-MAP
```

Bước 7: ACL cho lưu lượng mã hóa

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

4. Cấu hình Router B

Bước 1: Cấu hình IP cho các giao diện

```
interface gig0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown

interface gig0/1
 ip address 10.1.1.2 255.255.255.252
 no shutdown
```

Bước 2: Định tuyến tĩnh

```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

Bước 3: Cấu hình ISAKMP

```
crypto isakmp policy 10
 encryption aes
 hash sha256
 authentication pre-share
 group 2
crypto isakmp key vpn123 address 10.1.1.1
```

Bước 4: Tạo IPSec Transform Set

```
crypto ipsec transform-set VPN-TRANSFORM esp-aes esp-sha256-hmac
 mode tunnel
```

Bước 5: Tạo Crypto Map

```
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set VPN-TRANSFORM
 match address 102
```

Bước 6: Áp dụng Crypto Map vào Giao Diện WAN

```
interface gig0/1
 crypto map VPN-MAP
```

Bước 7: ACL cho lưu lượng mã hóa

```
access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

5. Kiểm tra kết nối

1. Ping giữa PC1 (192.168.1.x) và PC2 (192.168.2.x):
    - Ping từ PC1 đến PC2 và ngược lại.
    - Nếu cấu hình đúng, các gói tin sẽ được mã hóa qua IPSec VPN.
2. Kiểm tra trạng thái VPN trên Router:
    - Lệnh kiểm tra:-show crypto isakmp sa

-show crypto ipsec sa

3.2 thử nghiệm theo mô hình client to site

1. Chuẩn bị môi trường

1. Công cụ cần thiết:

    GNS3: Mô phỏng môi trường mạng.

    Router hỗ trợ IPSec: (Cisco, Fortinet, Mikrotik, hoặc dùng Virtual PC).

    Client: Một máy ảo giả lập (VM), ví dụ: Ubuntu, Windows.

    Giao diện mạng khác nhau: Một interface cho public (WAN), một cho LAN.

2. Sơ đồ mạng:

    Client (PC giả lập): kết nối qua internet (public network) đến router trung tâm.

    Router trung tâm: thực hiện cấu hình IPSec.

    Server trong mạng LAN: Máy chủ mà client cần truy cập

```
Client (VPN) --- Internet --- (WAN) Router (LAN) --- Server
```

2. Cấu hình Router

1. Bước cấu hình cơ bản:

-Tạo interface cho WAN và LAN:

```
interface gig0/0
  ip address 192.168.1.1 255.255.255.0
interface gig0/1
  ip address 10.1.1.1 255.255.255.0
```

-Định tuyến:

```
ip route 0.0.0.0 0.0.0.0 <next_hop_wan>
```

2. Cấu hình IPSec:

-Tạo key (ISAKMP):

```
crypto isakmp policy 1
  encryption aes
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key <shared_key> address 0.0.0.0
```

-Cấu hình chính sách IPSec (transform-set);

```
crypto ipsec transform-set MY_TRANSFORM esp-aes esp-sha256-hmac
```

-Tạo cấu hình map VPN:

```
crypto map VPN-MAP 10 ipsec-isakmp
  set peer <client_ip>
  set transform-set MY_TRANSFORM
  match address 101
```

-Áp VPN Map vào interface:

```
interface gig0/0
  crypto map VPN-MAP
```

3.Định nghĩa ACL:

-Để xác định lưu lượng VPN được mã hóa:

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

3. Cấu hình Client

1. Công cụ client:

- Nếu sử dụng Windows: Cấu hình VPN qua tính năng IPSec Client.

- Nếu sử dụng Ubuntu:bash

```
sudo apt install strongswan
sudo vim /etc/ipsec.conf
```

2.Thêm cấu hình cho VPN Client:

```
conn vpn-test
    keyexchange=ikev2
    authby=secret
    left=<client_ip>
    right=<router_ip>
    auto=start
```

3.Kiểm tra kết nối từ Client:

```
ipsec up vpn-test
```

4. Kiểm tra và xác minh

1. Ping từ Client đến Server:
    - Chạy `ping <server_ip>` từ client để kiểm tra kết nối VPN.
2. Xác minh trạng thái IPSec trên Router:
    - Dùng lệnh:-show crypto isakmp

-sa show crypto ipsec sa

KẾT LUẬN

Qua quá trình triển khai và thử nghiệm giao thức IPSec trên GNS3 theo hai mô hình site-to-site và client-to-site, chúng tôi rút ra các kết luận sau:

1. Hiệu quả bảo mật của IPSec:

- IPSec đã chứng minh khả năng bảo mật mạnh mẽ, đảm bảo tính bí mật, toàn vẹn và xác thực của dữ liệu truyền qua mạng không tin cậy (Internet).

- Dữ liệu giữa hai site và từ client đến site đều được mã hóa hoàn toàn, ngăn chặn các tấn công như nghe lén (eavesdropping) và thay đổi dữ liệu.

2. Mô hình site-to-site:

- Ưu điểm: Phù hợp cho kết nối cố định giữa hai mạng LAN, giúp đảm bảo tính bảo mật dữ liệu xuyên suốt giữa hai tổ chức hoặc chi nhánh. Không yêu cầu cấu hình phức tạp trên từng máy trạm trong mạng LAN, giảm tải công việc quản trị.

- Nhược điểm: Thiết lập phụ thuộc vào thiết bị định tuyến hỗ trợ IPSec. Chỉ hiệu quả cho các kết nối cố định, không phù hợp với các người dùng di động.

3. Mô hình client-to-site:

- Ưu điểm: Đáp ứng nhu cầu của các nhân viên làm việc từ xa (remote) với khả năng truy cập bảo mật vào hệ thống mạng của tổ chức. Linh hoạt và dễ triển khai, chỉ cần cấu hình đúng trên client và thiết bị VPN server.

- Nhược điểm: Yêu cầu cài đặt phần mềm VPN client trên thiết bị người dùng. Hiệu suất có thể bị ảnh hưởng do phụ thuộc vào kết nối Internet của từng client.

4. Tổng kết

- IPSec là giải pháp bảo mật mạng đáng tin cậy, đáp ứng được nhiều kịch bản mạng khác nhau. Mô hình **site-to-site** phù hợp cho tổ chức có nhiều chi nhánh, trong khi **client-to-site** phù hợp cho tổ chức muốn hỗ trợ làm việc từ xa.

- Việc triển khai và kiểm thử IPSec trên GNS3 giúp chuẩn bị tốt về cấu hình, tối ưu hóa chi phí và giảm thiểu rủi ro trước khi áp dụng trong thực tế