|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  Logo HvKTMM |
| THỰC TẬP TỐT NGHIỆP  **BÁO CÁO THỰC TẬP TỐT NGHIỆP**  **TRIỂN KHAI HỆ THỐNG SỬ DỤNG IPSEC CHO ADG** |
| Ngành: An toàn thông tin  Mã số: 7.48.02.02  *Sinh viên thực hiện*:  **Nguyễn Đức Tùng**  Lớp: AT13I  *Đơn vị thực tập:*  **Công ty ADG**  *Người quản lý thực tập*:  **Gv. Hoàng Thu Phương**  Khoa ATTT – Học viện KTMM  **Hà Nội - 2021** |

[**Lời mở đầu** 2](#_Toc66901368)

[I. Giới thiệu về cơ sở thực tập. 2](#_Toc66901370)

[1. Loại hình doanh nghiệp. 2](#_Toc66901371)

[2. Khái quát quá trình hình thành và phát triển. 2](#_Toc66901372)

[3. Cơ cấu tổ chức, chức năng của từng bộ phận, cơ cấu nguồn lực. 3](#_Toc66901373)

[3.1. Cơ cấu tổ chức. 3](#_Toc66901374)

[3.2. Chức năng, nhiệm vụ từng bộ phận. 3](#_Toc66901375)

[4. Các lĩnh vực kinh doanh, sản xuất. 5](#_Toc66901376)

[5. Chiến lược, định hướng phát triển trong thời gian tới. 5](#_Toc66901377)

[II. Phân tích các nguy cơ mất an toàn thông tin và đề xuất giải pháp khắc phục 6](#_Toc66901378)

[1. Khảo sát hiện trạng hạ tầng công nghệ thông tin và an toàn thông tin. 6](#_Toc66901379)

[2. Phân tích làm rõ các nguy cơ mất an toàn thông tin đối với hạ tầng công nghệ thông tin hiện có 7](#_Toc66901380)

[3. Phân tích, đánh giá các giải pháp an toàn thông tin hiện có. 8](#_Toc66901381)

[4. Đề xuất các giải pháp nhằm khắc phục hạn chế, giúp nâng cao mức độ an toàn. 8](#_Toc66901382)

[5. Triển khai thử nghiệm và đánh giá 8](#_Toc66901383)

[5.1. Triển khai 8](#_Toc66901384)

[5.2. Đánh giá kết quả 10](#_Toc66901385)

# **Lời mở đầu**

# **Nội dung**

## Giới thiệu về cơ sở thực tập.

### Loại hình doanh nghiệp.

- Công Ty Cổ phần Đầu Tư và Phát Triển Công Nghệ Quốc Gia ADG là nhà phân phối giá trị gia tăng cho các thương hiệu hàng đầu toàn cầu, cung cấp các giải pháp công nghệ thông tin cho các doanh nghiệp, cơ quan chính phủ, tổ chức và cá nhân.

- Công Ty Cổ phần Đầu Tư và Phát Triển Công Nghệ Quốc Gia ADG (ADG National Investment and Technology Development Corporation) là công ty có hơn 14 năm kinh nghiệm trong lĩnh vực kinh doanh phân phối các thiết bị phần cứng, phần mềm, thiết bị văn phòng, thiết bị tự động hoá và viễn thông của gần 20 hãng công nghệ nổi tiếng thế giới. Với đội ngũ kỹ sư phần cứng và chuyên gia phát triển phần mềm có năng lực và dày dan kinh nghiệm; ADG đã cung cấp được nhiều giải pháp ứng dụng mới, thiết kế riêng biệt cho từng tổ chức và doanh nghiệp nhằm giúp họ hóa tối ưu hóa quy trình vận hành.

### Khái quát quá trình hình thành và phát triển.

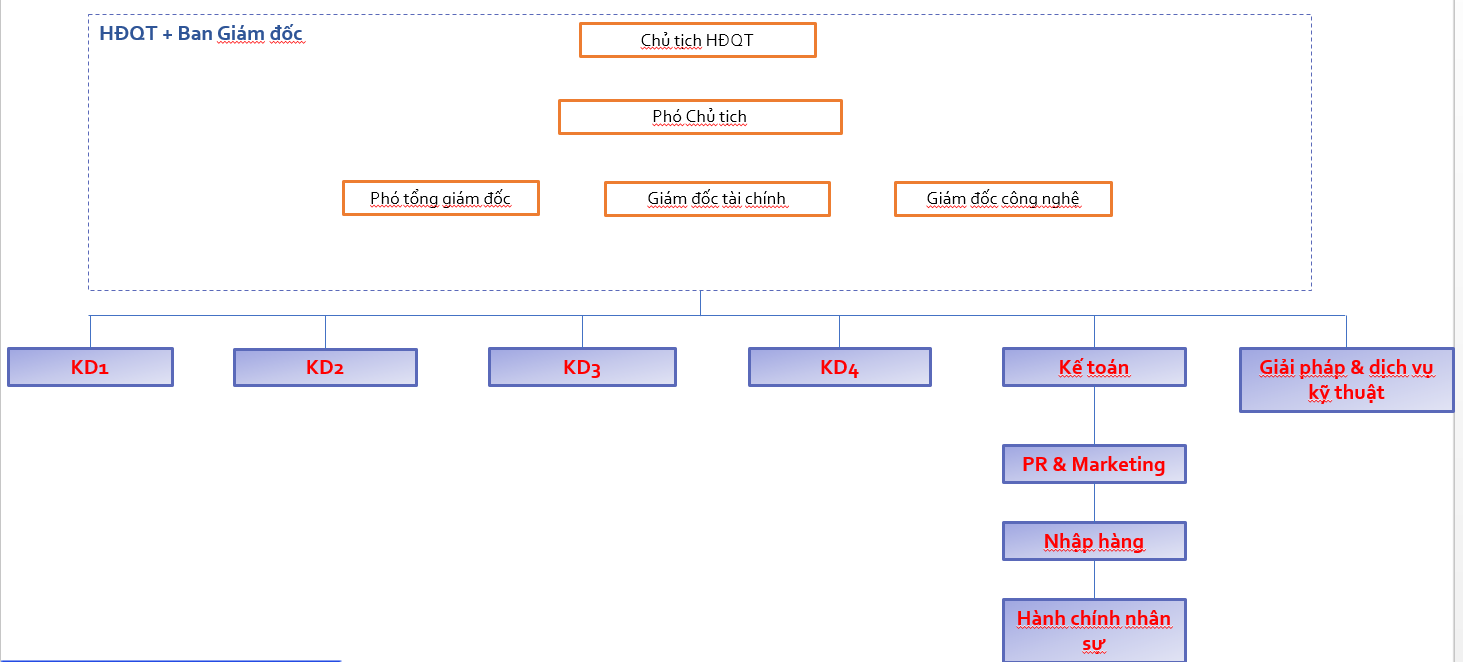
- Công ty ADG được thành lập năm 2006 với trụ sở chính đặt tại Hà Nội

- Cho đến nay, công ty đã mở thêm 3 chi nhánh tại Đà Nẵng, Hồ Chí Minh và Cần Thơ

- Hiện tại, công ty có trên 160 thành viên.

### Cơ cấu tổ chức, chức năng của từng bộ phận, cơ cấu nguồn lực.

#### Cơ cấu tổ chức.



1. Cơ cấu tổ chức công ty ADG

- Được thành lập vào năm 2006, đến nay, ADG đã có một bộ máy điều hành vững chắc gồm hơn 160 thành viên làm việc trong các phòng ban khác nhau, bao gồm Hội đồng quản trị công ty, ban giám đốc và các phòng ban kinh doanh cũng như giải pháp, kỹ thuật dịch vụ,…

#### Chức năng, nhiệm vụ từng bộ phận.

##### Hội đồng quản trị và ban giám đốc.

- Đây là “bộ máy chủ chốt” của công ty, gồm 5 thành viên.

- Đóng vai trò chung là thiết lập các chính sách, định hướng chiến lược cho công ty cũng như giám sát toàn bộ quản lý của công ty, đảm bảo việc vận hành.

- Mỗi thành viên trong HĐQT và ban giám đốc chịu trách nghiệm điều hành từng mảng khác nhau như công nghệ, kinh doanh hay tài chính,…

##### Các phòng ban kinh doanh

- Vì lĩnh vực chính của công ty là đầu tư và phát triển nên các phòng ban kinh doanh là không thể thiếu.

- Công ty chia thành 4 phòng ban kinh doanh chính với hơn 50 nhân sự.

- Các phòng ban kinh doanh chịu trách nhiệm làm việc với các đối tác cũng như khách hàng khác nhau như Oracle, Dell, Fujitsu, …

- Phòng kinh doanh cũng giữ vai trò thúc đẩy, phân phối các sản phẩm, dịch vụ của đối tác dến các đại lý.

##### Phòng kế toán.

- Phòng gồm 5-6 thành viên đóng vai trò thực hiện những công việc về nghiệp vụ chuyên môn tài chính kế toán theo đúng quy định của Nhà nước.

- Theo dõi, phản ánh sự vận động vốn kinh doanh của công ty và cố vấn cho Ban giám đốc.

- Quản lý công nợ, quản lý vốn vay.

##### Phòng PR & Marketing.

- Đóng vai trò quan trọng trong việc quản bá sản phẩm mà công ty kinh doanh đến khách hàng, cũng như nghiên cứu, xác định nhu cầu người dùng trên thị trường, từ đó cố vấn cho Ban giám đốc để có những chiến lược phát triển, mở rộng sản phẩm cho công ty.

##### Nhập hàng.

- Đây là bộ phận quản lý kho cũng như việc nhập hàng, bảo vệ thiết bị, hàng hóa của công ty.

- Bộ phận đóng vai trò lập và hoàn thiện phiếu nhập kho bằng cách xử lý các yêu cầu đến từ các phòng kinh doanh.

- Làm việc với các nhà cung cấp để tìm kiếm nguồn hàng hóa mới cho công ty.

- Quản lý hàng tồn kho và bảo quản hàng hóa theo tiêu chuẩn quy định.

##### Phòng hành chính nhân sự.

- Xây dựng cơ cấu nhân sự cho các phòng ban trong công ty. Tham mưu cho Ban giám đốc về việc sắp xếp, bố trí và phát triển nhân sự thông qua việc phân tích cơ cấu, tổ chức, đánh giá kết quả công việc và năng lực nhân sự.

- Xây dựng quy chế tiền lương, thưởng, nội quy lao động và các quy chế làm việc và quy trình, quy chế trong công tác tuyển dụng, đào tạo, bổ nhiệm,…

- Công tác hành chính xây dựng quy chế và thực hiện các công tác văn thư, lưu trữ, quản lý hồ sơ pháp lý của công ty. Thực hiện các thủ tục hành chính pháp lý, soạn thảo các văn bản hành chính, tổ chức các cuộc họp cũng như sự kiện hàng năm của doanh nghiệp.

- Lên kế hoạch mua sắm, quản lý, hướng dẫn sử dụng tài sản chung của doanh nghiệp, phối hợp thực hiện việc kiểm kê và thanh lý tài sản.

##### Giải pháp và dịch vụ kỹ thuật.

- Tư vấn và hỗ trợ khách hàng các vấn đề liên quan đến kĩ thuật. Cài đặt, hướng dẫn khách hàng sử dụng sản phẩm. Bảo hành hoặc đổi trả nếu gặp sản phẩm lỗi.

- Nghiên cứu các giải pháp công nghệ thông tin đang thịnh hành, tư vấn Ban giám đốc các ứng dụng liên quan đến quản trị doanh nghiệp, an toàn thông tin.

- Nghiên cứu và đào tạo các sản phẩm mới cho các phòng ban kinh doanh.

### Các lĩnh vực kinh doanh.

- Công ty có một hệ sinh thái công nghệ bao gồm: Phần mềm doanh nghiệp; máy tính, các thiết bị mạng, lưu trữ; Hạ tầng trung tâm dữ liệu và an ninh mạng.

- Sản phẩm hiện nay công ty kinh doanh rất đa dạng như:

* Thương hiệu Dell: PC, laptop, server, thiết bị lưu trữ, giải pháp bảo vệ dữ liệu,…
* Thương hiệu Fujitsu: Màn hình tương tác, máy chủ, thiết bị lưu trữ, giải pháp bảo vệ dữ liệu, thiết bị scan tốc độ cao, thiết bị bảo mật tĩnh mạch lòng bàn tay,…
* Thương hiệu NetApps: Các sản phẩm lưu trữ, siêu hội tụ và bảo vệ dữ liệu,…

### Chiến lược, định hướng phát triển trong thời gian tới.

- Mở rộng đa dạng hóa sản phẩm.

- Kêu gọi đầu tư vốn từ các nguồn quỹ mở.

- Áp dụng AI vào quản trị hệ thống.

- Thu hút các nhân tài.

## Phân tích các nguy cơ mất an toàn thông tin và đề xuất giải pháp khắc phục

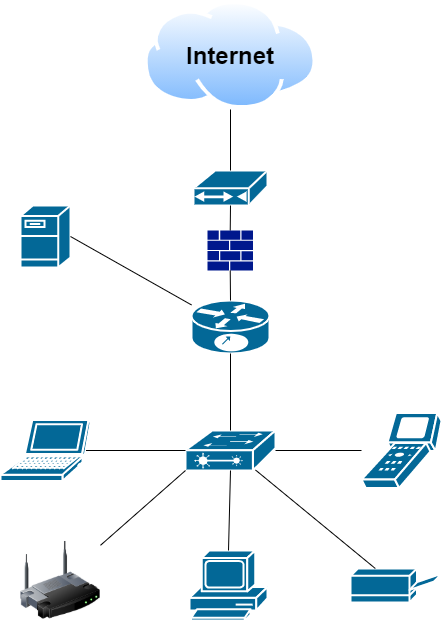
### Khảo sát hiện trạng hạ tầng công nghệ thông tin và an toàn thông tin.

- An toàn thông tin đóng vai trò quan trọng trong việc bảo vệ dữ liệu của người dùng trong hệ thống công ty ADG.

- Nhìn chung, hệ thống mạng của công ty được thiết kế khá đơn giản nhưng vẫn đáp ứng đủ nhu cầu của người dùng trong hệ thống công ty.

- Các máy trạm, máy tính cá nhân đều được cài đặt những phần mềm diệt virus.

- Vì nguồn lực cho việc phát triển, nghiên cứu an toàn thông tin còn hạn hẹp, nên trang thiết bị phần cứng còn hạn chế, phần mềm bảo mật mới dừng ở các sản phẩm phổ thông.



Mô hinh mạng hệ thống công ty ADG

### Phân tích làm rõ các nguy cơ mất an toàn thông tin đối với hạ tầng công nghệ thông tin hiện có.

- Tuy hệ thống của công ty hoạt động khá ổn định nhưng cũng không thể tránh khỏi những rủi ro từ bên ngoài.

- Việc dùng một con server để cho nhiều mục đích khác nhau như chia sẻ tài nguyên,quản lý người dùng… ta thấy được nguy cơ tiềm ẩn mất an toàn là khá cao nếu hacker chiếm quyền điều khiển của toàn bộ hệ thống.

- Đi tiếp vào trong hệ thống mạng từng phòng ban, ta thấy các phòng ban vẫn đang sử dụng chung một hệ thống mạng mà chưa chia thành các VLAN cụ thể, điều này dẫn tới việc các phòng ban có thể vô tình làm lộ dữ liệu nhạy cảm bên trong công ty.

- Những chính sách an toàn trong ADG còn khá “lỏng lẻo” ví dụ như đặt password cho máy tính cá nhân, hoặc đặt password đơn giản, tắt máy trước khi về,download những file không có bản quyền, file không có nguồn gốc… Tuy đây là những việc làm nhỏ và mất ít thời gian, nhưng lại rất cần thiết đối với việc an toàn trong một hệ thống.

- Vẫn chưa thường xuyên kiểm thử, kiểm tra định kì hệ thống mạng trong công ty như rà soát log firewall, rà soat log server,… Điều này có thể dẫn tới nguy cơ tiềm ẩn trong hệ thống mạng công ty.

- Những phần mềm như quét lỗ hổng, quét mạng không dây, nhận dạng cổng và dịch vụ mạng còn thiếu sót nhiều.

- Nhiều nhân viên trong công ty tắt cập nhật cho những phiên bản hệ điều hành mới. Điều này tuy sẽ không gây mất thời gian cho nhân viên, nhưng lại là 1 nguy cơ cao gây mất an toàn thông tin. Đó là việc những phần mềm Antivirus, anti malware sẽ không được cập nhật thường xuyên dẫn tới việc sẽ khó có thể phát hiện được những trình, những tệp tin độc hại.

- Dữ liệu trên máy chủ, máy tính cá nhân của ADG hiện chưa an toàn vì không được mã hóa nội dung kể cả khi đi trên đường truyền.

### Phân tích, đánh giá các giải pháp an toàn thông tin hiện có.

- Hiện nay, công ty đã và đang tuyên truyền về an toàn thông tin cũng như tầm quan trọng của nó đối với dữ liệu bảo mật của công ty nhằm nâng cao ý thức của mỗi thành viên trong công ty.

- Bổ sung thêm những chính sách an toàn thông tin như đặt mật khẩu phức tạp hoặc thường xuyên trong việc rà soát các file nhật ký trong hệ thống.

### Đề xuất các giải pháp nhằm khắc phục hạn chế, giúp nâng cao mức độ an toàn.

- Trong hệ thống mạng trong công ty, có thể coi là còn khá đơn giản nhưng cũng còn phải phụ thuộc vào nhu cầu, ngân sách cũng như nguồn lực phía công ty. Việc đưa ra những giải pháp tốn nhiều chi phí trong thời điểm hiện tại là chưa cần thiết vì có thể chia thành nhiều giai đoạn hoàn thiện theo thời gian.

- Nếu kinh phí cho phép thì nên bổ sung thêm 1 con server để tránh việc đầy tài nguyên và sẵn sàng sao lưu dự phòng nếu cần thiết.

- Bổ sung các luật trong tường lửa để có thể phòng tránh tối đa rủi ro đến an toàn thông tin của công ty.

- Việc cần thiết là rà soát định kì các file nhật ký trong hệ thống, như server, firewall,…

- Thường xuyên kiểm tra, giám sát về việc tuân thủ những chính sách an toàn thông tin của nhân viên đối với công ty.

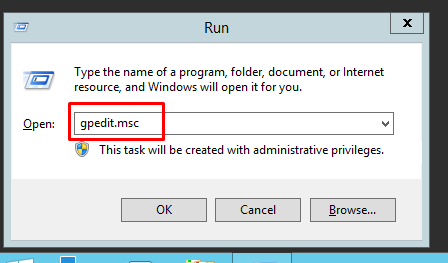
- Tại hệ thống máy chủ và máy tính có dữ liệu nhạy cảm, có dữ liệu cần được chia sẻ; tại các thiết bị lưu trữ cần phải tiến hành mã hóa nội dung. Giải pháp Ipsec sẽ được triển khai tại các hệ thống máy chủ và máy người dùng cũng như các thiết bị mạng phải được cấu hình.

### Triển khai thử nghiệm và đánh giá

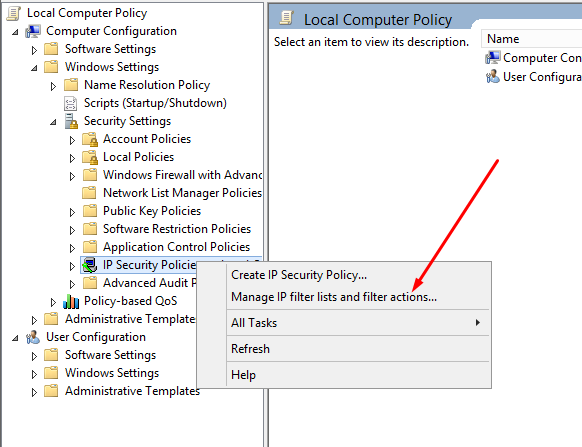
#### Triển khai

Cài đặt thử nghiệm hệ thống với giao thức Ipsec cho máy windows server 2012 và windows 10 (mô phỏng trên Vmware)

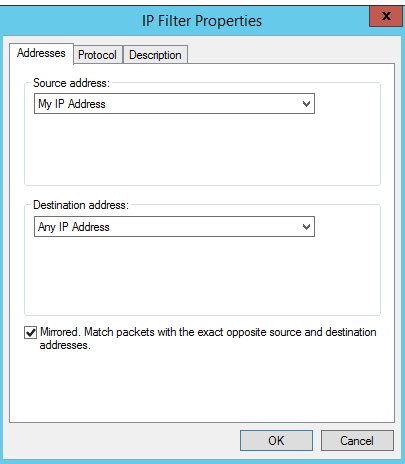
Bước 1: Trên windows server 2012, gõ lệnh gpedit.msc



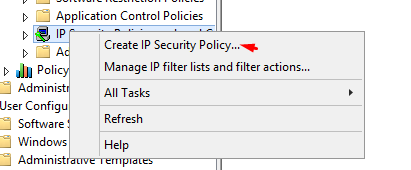
Bước 2: Trong phần IP Security Policies, chọn Manage IP filter lists and filter actions



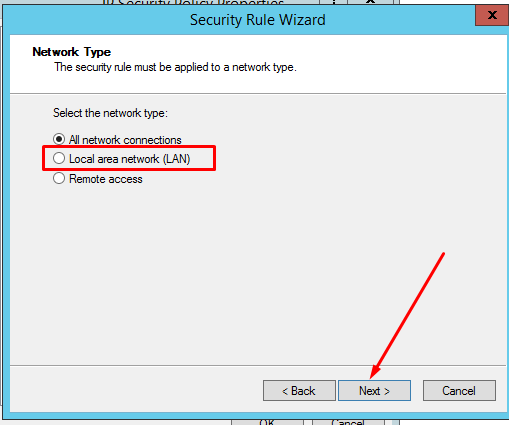
Bước 3: Lọc địa chỉ nguồn và địa chỉ đích cần mã hóa trên đường truyền



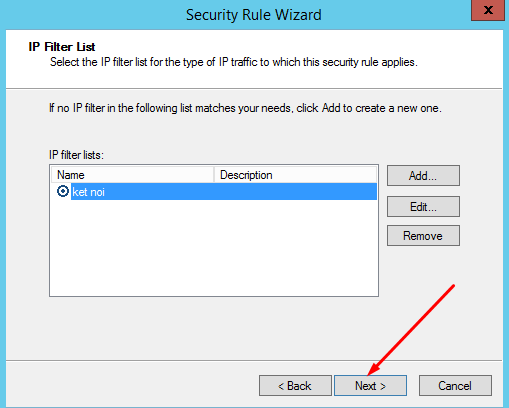
Bước 6: Chọn Create Ipsec Policy để tiến hành tạo chính sách



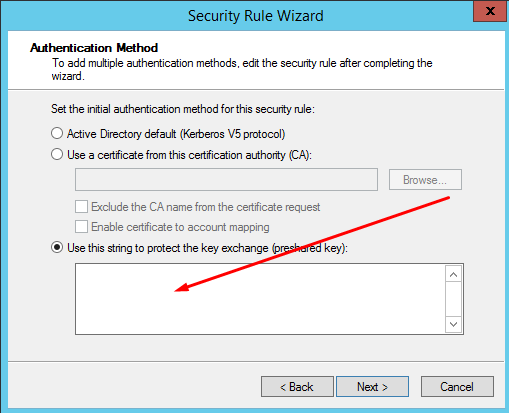
Bước 7: Chọn kiểu mạng là LAN (Mạng cục bộ)



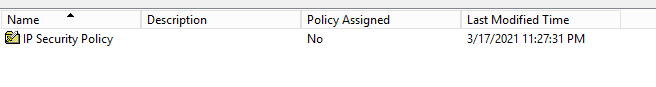
Bước 8: Chọn kiểu fitter vừa tạo ở bên trên



Bước 9: Nhập Preshared Key

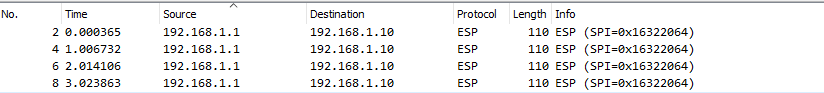


Bước 10: Kết quả



Tiếp theo bật chế độ kích hoạt cho chính sách vừa tạo, đồng thời làm tương tự trên các máy tính cá nhân.

Bước 11: Sau khi làm tương tự trên máy windows 10 thành công, tiến hành ping và chặn bắt gói tin bằng phần mềm Wireshark:



Qua đây em thấy các giao thức dùng trong conversation này là IPsec(esp) chứ không còn là ICMP nữa, giao thức này cung cấp tính năng bảo mật.

Bước 12: Tiếp tục thực nghiệm trong vấn đề truyền file:

1. Truyền file không dùng giao thức IPsec

C:\Users\admin\OneDrive\Desktop\Thực tập báo cáo\Screenshot_2.png

2. Truyền file dùng giao thức Ipsec

C:\Users\admin\OneDrive\Desktop\Thực tập báo cáo\Screenshot_3.png

Dữ liệu người dùng sẽ được bảo mật trong môi trường truyền tin nếu sử dụng giao thức Ipsec.

#### Kết luận.

Giao thức ESP cung cấp phần mã hóa của IPSec, đảm bảo tính bảo mật của lưu lượng dữ liệu giữa các thiết bị. ESP mã hóa các gói dữ liệu/payload, xác thực payload và nguồn gốc của nó trong bộ giao thức IPSec. Giao thức này xáo trộn lưu lượng truy cập Internet một cách hiệu quả, để bất kỳ ai nhìn vào tunnel cũng đều không thể thấy bất cứ gì trong đó.

Nhờ sự giúp đỡ tận tình của các chú, các anh và mọi người trong công ty, em đã triển khai và báo cáo các bước để áp dụng giao thức Ipsec vào thực tế. Tuy nhiên vẫn cần phải có sự thông qua của ban lãnh đạo để thực hiện với toàn bộ các máy tính trong công ty và sau đó mới có kế hoạch triển khai cụ thế.

# **Kết luận**