

Các cơ chế an toàn trên hệ điều hành WINDOWS

MỤC LỤC

| | |
|---|----|
| DANH MỤC CÁC HÌNH VẼ | 2 |
| TÓM TẮT NỘI DUNG | 3 |
| I. Giới thiệu..... | 4 |
| 1.1. Hệ điều hành Windows – một trong những hệ điều hành phổ biến nhất trên thế giới..... | 4 |
| 1.2. Tầm quan trọng của việc bảo vệ dữ liệu và thông tin cá nhân trong thời đại số..... | 5 |
| 1.3. Giới thiệu về các cơ chế bảo vệ có sẵn trên Windows..... | 5 |
| II. Cơ chế xác thực và quyền truy cập | 8 |
| 2.1. Một số cơ chế xác thực phổ biến của Windows | 8 |
| 2.2. Quản lý quyền truy cập cho người dùng và nhóm người dùng | 9 |
| 2.3. Cách Windows quản lý và bảo vệ các quyền truy cập quan trọng như quyền quản trị viên | 9 |
| III. Cơ chế bảo vệ trước phần mềm độc hại 3.1. Windows Defender, công cụ bảo vệ tích hợp sẵn trong Windows..... | 10 |
| 3.2. Cơ chế hoạt động của Windows Defender | 11 |
| 3.3. Tầm quan trọng của việc cập nhật định kỳ để bảo vệ hệ thống khỏi các mối đe dọa mới..... | 12 |
| IV. Cơ chế bảo vệ dữ liệu..... | 12 |
| 4.1. Giới thiệu về BitLocker, công cụ mã hóa ổ đĩa của Windows | 13 |
| 4.2. Cách hoạt động và lợi ích của việc sử dụng BitLocker | 13 |
| 4.3. Phương pháp sao lưu và phục hồi dữ liệu trên Windows | 14 |
| V. Cơ chế bảo vệ tường lửa và mạng..... | 15 |
| 5.1. Giới thiệu về tường lửa của Windows(Windows Firewall) | 15 |
| 5.2. Cách tường lửa Windows giúp bảo vệ hệ thống | 16 |
| 5.3. Các cơ chế bảo vệ mạng khác: | 17 |
| VI. Thực nghiệm | 17 |

| | |
|--|-----------|
| 6.1. Cơ chế kiểm soát truy cập..... | 17 |
| Mục tiêu | 17 |
| Bối cảnh..... | 17 |
| Tài nguyên yêu cầu | 18 |
| Kiểm soát truy cập | 18 |
| 6.2. Bảo vệ tài khoản | 26 |
| Mục tiêu | 26 |
| 6.3. Tường lửa | 27 |
| Mục tiêu | 27 |
| Bối cảnh..... | 27 |
| Tài nguyên yêu cầu | 27 |
| VII. Kết luận..... | 34 |
| 7.1. Tầm quan trọng của việc hiểu và áp dụng đúng các cơ chế bảo vệ của Windows.... | 35 |
| 7.2. Khuyến nghị về việc tiếp tục cập nhật kiến thức về an ninh mạng và bảo vệ hệ thống | 35 |
| CÀI ĐẶT MÔI TRƯỜNG MÁY ẢO | 37 |
| 1. Cài đặt công cụ Virtual Box hoặc VMWare, máy ảo Windows 10 và Windows Server 2012 | 37 |
| 2. Tạo Domain Server | 39 |
| 3. Cách join domain từ Máy client với máy Server | 41 |

DANH MỤC CÁC HÌNH VẼ

| |
|---|
| Hình 1: Công cụ Windows Defender được tích hợp trực tiếp vào Windows |
| Hình 2: Firewall của Windows |
| Hình 3: Yêu cầu phải đăng nhập tài khoản của Admin thì hành động này mới thực hiện thành công |

| | |
|---|--|
| Hình 4: BitLocker yêu cầu mã PIN để unlock device | |
| Hình 5: Windows Update | |
| Hình 6: BitLocker | |
| Hình 7: Tường lửa | |
| Hình 8: Server Manager | |
| Hình 9: Cách add user vào hệ thống | |
| Hình 10: Tạo file .text bằng Notepad | |
| Hình 11: Cách share, set Read-Only cho folder và phân quyền cho user | |
| Hình 12: Thông báo người dùng user2 không thể chỉnh sửa file | |
| Hình 13: Permissions mặc định khi thêm user có quyền với file hoặc folder | |
| Hình 14: Gán địa chỉ IP tại Scope | |
| Hình 15: Ping thành công từ máy Client đến máy Server khi Server cho phép connect | |
| Hình 16: Thay đổi Rule bằng cách vào Properties của Rule đó | |
| Hình 17: Ping thất bại từ máy Client đến Server khi Server chặn connection .. | |
| Hình 18: Dán đường dẫn của một ứng dụng nào đó tại Program của Outbound Rules | |
| Hình 19: Block connect Internet của một ứng dụng MS Edge mà máy client đang sử dụng | |
| Hình 20: Máy Client (192.168.1.12) đã bị chặn truy cập Internet tại MS Edge .. | |
| Hình 21: VirtualBox | |
| Hình 22: Tắt tường lửa..... | |
| Hình 23: Set IP cho máy Server | |
| Hình 24: Add role Active Directory Domain Services | |

TÓM TẮT NỘI DUNG

- Phần I: Tổng quan về hệ điều hành Windows: Phần này giới thiệu về hệ điều hành Windows, tầm quan trọng của việc bảo vệ dữ liệu thông tin cá nhân và

giới thiệu các cơ chế an toàn bảo mật có sẵn trên Windows.

- Phần II -> V: Phần này nói về cách thức hoạt động của các cơ chế an toàn.
- Phần VI: Phần này chú trọng vào việc thực hành các cơ chế an toàn: mô tả quá trình thành lập hệ thống an toàn và kết quả của nó.
 - Kiểm soát truy cập
 - Tường lửa
 - Bảo vệ tài khoản
- Phần VII: Kết luận: Tầm quan trọng của việc hiểu và áp dụng đúng các cơ chế bảo vệ của Windows. Khuyến nghị về việc tiếp tục cập nhật kiến thức về an ninh mạng và bảo vệ hệ thống

I. Giới thiệu

1.1. Hệ điều hành Windows – một trong những hệ điều hành phổ biến nhất trên thế giới

Windows là một hệ điều hành được phát triển và phân phối bởi Microsoft, một công ty công nghệ lớn có trụ sở tại Redmond, Washington, Hoa Kỳ. Từ khi được giới thiệu lần đầu vào năm 1985, Windows đã trở thành một trong những hệ điều hành phổ biến nhất trên thế giới, đặc biệt là trong môi trường văn phòng và gia đình.

Một số đặc điểm nổi bật của Windows:

- Giao diện đồ họa người dùng (Graphical User Interface - GUI): Windows sử dụng một giao diện đồ họa người dùng dễ sử dụng, cho phép người dùng tương tác với máy tính thông qua các biểu tượng, cửa sổ và menu thay vì phải nhập các lệnh văn bản.
- Tính tương thích rộng rãi: Windows tương thích với hầu hết các ứng dụng phần mềm và phần cứng máy tính. Ví dụ như các ứng dụng văn phòng như Microsoft Office, các trình duyệt web như Chrome Firefox,
...
- Phiên bản đa dạng: Windows có nhiều phiên bản khác nhau, từ phiên bản dành cho người dùng cá nhân như Windows Home, đến phiên bản dành cho doanh nghiệp như Windows Pro và Windows Enterprise.

- Bảo mật và quản lý: Windows cung cấp nhiều cơ chế bảo vệ và quản lý hệ thống, bao gồm quản lý quyền truy cập, cập nhật bảo mật, công cụ chống virus, và các cơ chế bảo vệ dữ liệu như BitLocker.
- Windows luôn được cập nhật và cải tiến, với các phiên bản mới nhất luôn được phát hành để cung cấp các tính năng mới và cải thiện hiệu suất, bảo mật và tính ổn định.

1.2. Tầm quan trọng của việc bảo vệ dữ liệu và thông tin cá nhân trong thời đại số

Trong thời đại số hiện nay, việc bảo vệ dữ liệu và thông tin cá nhân đã trở thành một vấn đề cực kỳ quan trọng và cần thiết. Dưới đây là một số lý do để minh họa cho điều này:

Thông tin cá nhân như tên, địa chỉ, số điện thoại, và thông tin tài chính (như số tài khoản ngân hàng hoặc thông tin thẻ tín dụng) có thể bị lạm dụng nếu rơi vào tay người xấu. Các hành vi lạm dụng thông tin cá nhân có thể bao gồm gian lận tài chính, chiếm đoạt tài khoản trực tuyến, hoặc thậm chí là đe dọa an ninh cá nhân.

Quyền riêng tư là một quyền cơ bản của con người. Trong thế giới số hóa, việc bảo vệ dữ liệu cá nhân từ sự xâm nhập không mong muốn cũng chính là việc bảo vệ quyền riêng tư của bản thân mỗi người dùng.

Tội phạm mạng ngày càng tăng, với các hình thức tấn công ngày càng tinh vi. Việc bảo vệ dữ liệu không chỉ giúp bảo vệ thông tin cá nhân, mà còn giúp ngăn chặn các cuộc tấn công này.

Nhiều quốc gia và khu vực đã ban hành luật về bảo mật dữ liệu, yêu cầu các tổ chức và doanh nghiệp bảo vệ dữ liệu khách hàng và thông tin cá nhân. Việc không tuân thủ có thể dẫn đến các hậu quả pháp lý nghiêm trọng.

Việc tăng cường bảo vệ dữ liệu và thông tin cá nhân không chỉ là trách nhiệm của các tổ chức và doanh nghiệp mà cũng là trách nhiệm của mỗi cá nhân. Để đạt được điều này, chúng ta cần nâng cao nhận thức, học cách sử dụng công nghệ một cách an toàn, và ứng dụng các biện pháp bảo vệ dữ liệu phù hợp.

1.3. Giới thiệu về các cơ chế bảo vệ có sẵn trên Windows

Hệ điều hành Windows cung cấp nhiều cơ chế bảo vệ để giúp người dùng bảo vệ dữ liệu và thông tin cá nhân của mình.

Một số cơ chế bảo vệ quan trọng

- Windows Defender:

Windows Defender là một công cụ chống phần mềm độc hại được tích hợp trực tiếp vào hệ điều hành Windows. Nó cung cấp bảo vệ thời gian thực khỏi các mối đe dọa như virus, malware, spyware và ransomware.



Hình 1: Công cụ Windows Defender được tích hợp trực tiếp vào Windows

- Firewall của Windows:

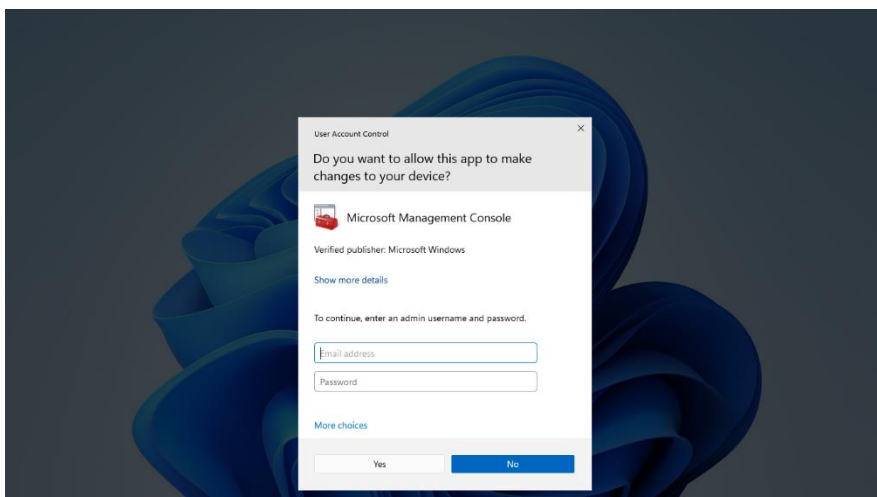
Firewall giúp ngăn chặn truy cập không được phép vào máy tính của người dùng từ Internet hoặc mạng nội bộ. Nó có thể được cấu hình để cho phép hoặc từ chối truy cập vào các ứng dụng cụ thể.



Hình 2: Firewall của Windows

- Control User Account (UAC):

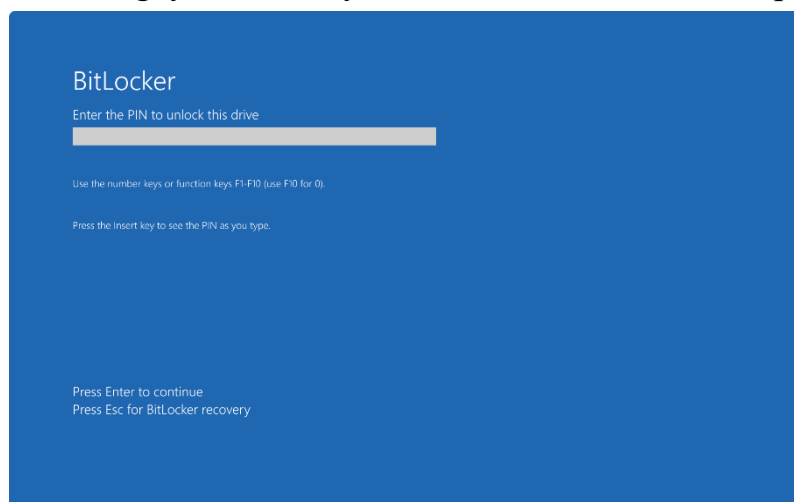
UAC giúp ngăn chặn các thay đổi không mong muốn đối với hệ thống của người dùng bằng cách yêu cầu xác nhận hoặc mật khẩu quản trị viên khi thực hiện các hành động có thể ảnh hưởng đến hoạt động của máy tính.



Hình 3: Yêu cầu phải đăng nhập tài khoản của Admin thì hành động này mới thực hiện thành công

- BitLocker:

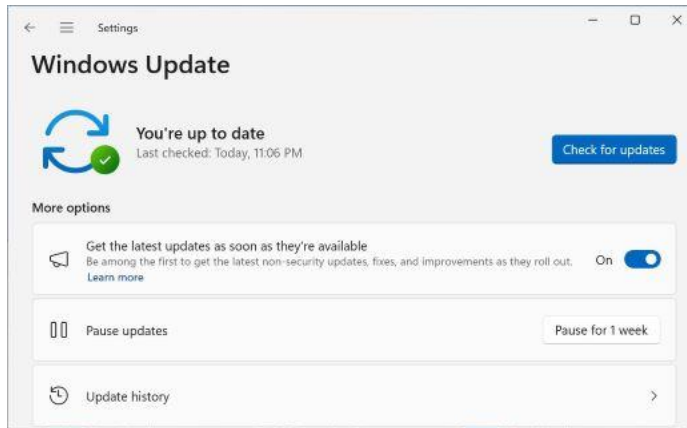
BitLocker là một công cụ mã hóa ổ đĩa giúp bảo vệ dữ liệu của người sử dụng khỏi truy cập trái phép. Nó mã hóa toàn bộ ổ đĩa, giúp dữ liệu của người dùng an toàn ngay cả khi máy tính bị mất hoặc bị đánh cắp.



Hình 4: BitLocker yêu cầu mã PIN để unlock device

- Windows Update:

Windows Update là một cơ chế giúp cập nhật hệ điều hành, bao gồm các cập nhật bảo mật. Việc giữ hệ thống được cập nhật là một phần quan trọng của việc bảo vệ máy tính khỏi các mối đe dọa.



Hình 5: Windows Update

Các cơ chế này cung cấp một lớp bảo vệ cơ bản cho máy tính chạy Windows.

II. Cơ chế xác thực và quyền truy cập

2.1. Một số cơ chế xác thực phổ biến của Windows

Xác thực bằng mật khẩu: Đây là phương thức xác thực đơn giản và phổ biến nhất. Người dùng cần nhập đúng mật khẩu được thiết lập trước đó để truy cập vào hệ thống. Tuy nhiên, phương thức này dễ bị tấn công brute-force và phishing nếu mật khẩu không đủ mạnh.

Xác thực hai yếu tố: Phương thức này yêu cầu người dùng cung cấp hai loại bằng chứng để xác thực danh tính:

Yếu tố thứ nhất: Thông tin mà người dùng biết (mật khẩu).

Yếu tố thứ hai: Thông tin mà người dùng có (mã xác thực gửi qua điện thoại hoặc email).

Xác thực dựa trên mã PIN: Khác với mật khẩu truyền thống, mã PIN chỉ có thể được sử dụng trên thiết bị cụ thể mà người dùng đã thiết lập, giúp tăng cường bảo mật.

2.2. Quản lý quyền truy cập cho người dùng và nhóm người dùng

Xác định và phân loại dữ liệu: Xác định các loại dữ liệu quan trọng và phân loại chúng theo mức độ nhạy cảm và quyền riêng tư.

Thiết lập chính sách và quy trình: Xây dựng chính sách quản lý quyền truy cập, bao gồm nguyên tắc lưỡng cực, phân tách trách nhiệm và nguyên tắc trách nhiệm tối thiểu.

Xác thực người dùng: Sử dụng các phương pháp xác thực như tên người dùng/mật khẩu, mã thông báo (token), xác thực đa yếu tố (MFA) để xác nhận danh tính người dùng trước khi cấp quyền truy cập.

Phân quyền dựa trên vai trò (RBAC): Gán quyền truy cập dựa trên vai trò của người dùng, đảm bảo họ chỉ có quyền truy cập vào những tài nguyên cần thiết cho công việc của mình.

Quản lý danh sách kiểm soát truy cập (ACL): Áp dụng các danh sách kiểm soát truy cập để điều chỉnh quyền truy cập vào các tài nguyên cụ thể, như file, thư mục, hoặc mạng.

Kiểm tra và giám sát: Thực hiện kiểm tra định kỳ và giám sát hoạt động truy cập để phát hiện và ngăn chặn các hành vi không được phép và các mối đe dọa bảo mật.

Đánh giá và cập nhật: Liên tục đánh giá và cập nhật các chính sách, quy trình và cơ sở hạ tầng để đảm bảo rằng hệ thống quản lý quyền truy cập luôn hiệu quả và phù hợp với môi trường bảo mật.

2.3. Cách Windows quản lý và bảo vệ các quyền truy cập quan trọng như quyền quản trị viên

User Account Control (UAC): Yêu cầu sự xác nhận từ người dùng hoặc quản trị viên khi có hoạt động yêu cầu quyền quản trị viên, ngăn chặn các ứng dụng không xác thực khỏi việc thực thi các hoạt động không được phép.

Phân quyền người dùng và nhóm người dùng: Quản lý các tài khoản người dùng và nhóm người dùng để gán quyền truy cập phù hợp, bao gồm cả việc gán quyền quản trị viên cho các tài khoản cụ thể.

Group Policy: Thiết lập và quản lý các chính sách nhóm để cấu hình và áp dụng các quyền truy cập và cấu hình bảo mật trên nhiều máy tính trong một mạng.

Secure Boot và Virtualization-based Security (VBS): Sử dụng các tính năng bảo mật như Secure Boot và VBS để ngăn chặn các cuộc tấn công từ phần mềm độc hại và cải thiện bảo mật của hệ thống.

III. Cơ chế bảo vệ trước phần mềm độc hại

3.1. Windows Defender, công cụ bảo vệ tích hợp sẵn trong Windows

Windows Defender cung cấp bảo vệ thời gian thực chống lại virus, spyware, ransomware và các phần mềm độc hại khác. Nó quét và loại bỏ các tập tin, ứng dụng hoặc trang web có nguy cơ đe dọa hệ thống.

Windows Defender Firewall: Công cụ quản lý tường lửa của Windows Defender giúp ngăn chặn các kết nối mạng không an toàn và bảo vệ hệ thống khỏi các cuộc tấn công qua mạng.

Windows Defender SmartScreen: Công nghệ này bảo vệ trình duyệt Edge và cả Windows khi người dùng tải xuống hoặc truy cập vào các tài nguyên trực tuyến bằng cách phát hiện và cảnh báo về các trang web hoặc tập tin có thể không an toàn.

Windows Defender được tích hợp sẵn trong hệ điều hành Windows, điều này giúp đơn giản hóa việc bảo vệ máy tính và tự động cập nhật các định nghĩa

mới nhất để phòng ngừa các mối đe dọa mới.

Bên cạnh các chức năng cơ bản, Windows Defender cũng tích hợp các công nghệ bảo vệ tiên tiến như Machine Learning và phân tích hành vi để phát hiện và ngăn chặn các mối đe dọa phức tạp hơn.

3.2. Cơ chế hoạt động của Windows Defender

Windows Defender thực hiện quét hệ thống thường xuyên để phát hiện sớm các phần mềm độc hại như virus, spyware, trojan, ransomware và các loại mối đe dọa khác.

Các file và chương trình được mở và thực thi sẽ được phân tích thời gian thực để xác định xem chúng có hành vi độc hại hay không.

Windows Defender Firewall cung cấp tường lửa Windows Defender để kiểm soát các kết nối mạng vào và ra khỏi máy tính, ngăn chặn các cuộc tấn công mạng từ các máy chủ.

Windows Defender SmartScreen bảo vệ trình duyệt khỏi các trang web, ứng dụng và tập tin có thể không an toàn bằng cách phát hiện và cảnh báo người dùng trước khi họ truy cập hoặc tải xuống.

Khi phát hiện phần mềm độc hại, Windows Defender có thể xử lý nó bằng cách cách cách ly, xóa hoặc cảnh báo người dùng. Nó cũng cung cấp các báo cáo chi tiết về các mối đe dọa đã được xử lý và các hoạt động bảo vệ hệ thống.

3.3. Tầm quan trọng của việc cập nhật định kỳ để bảo vệ hệ thống khỏi các mối đe dọa mới

Các cập nhật định kỳ thường bao gồm các bản vá bảo mật (security patches) được phát hành bởi các nhà cung cấp hệ điều hành và phần mềm. Những bản vá này sửa các lỗ hổng bảo mật mới được phát hiện, giúp ngăn chặn các hacker và phần mềm độc hại tấn công vào các điểm yếu này.

Các nhà phát triển phần mềm độc hại luôn cố gắng tìm ra các lỗ hổng mới và phát triển các công cụ tấn công mới. Việc cập nhật định kỳ giúp hệ thống của bạn luôn có những phòng thủ mới nhất để đối phó với những mối đe dọa này.

Việc không cập nhật định kỳ có thể làm tăng nguy cơ mất dữ liệu quan trọng, thiệt hại do tấn công mạng hoặc sự ngừng hoạt động của hệ thống. Những tổn thất này không chỉ gây ảnh hưởng đến hoạt động kinh doanh mà còn có thể ảnh hưởng đến uy tín và niềm tin của khách hàng.

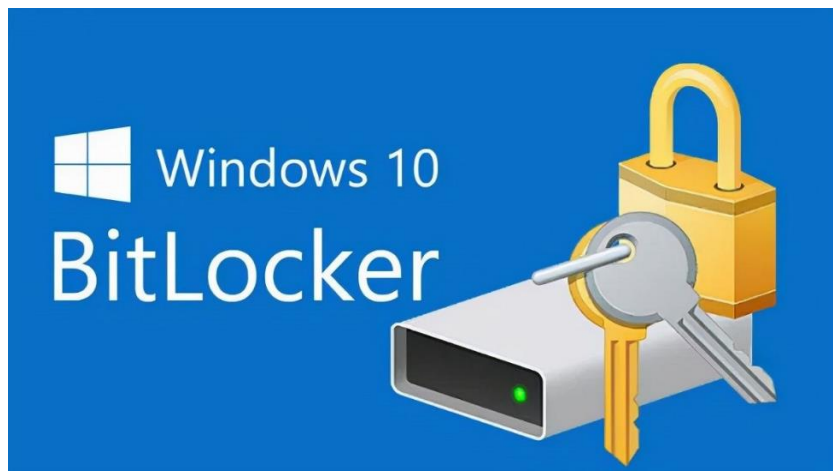
Các tổ chức thường phải tuân thủ các tiêu chuẩn và quy định về bảo mật như GDPR, PCI DSS, HIPAA. Việc cập nhật định kỳ giúp các tổ chức đáp ứng các yêu cầu này và giảm thiểu rủi ro về vi phạm quyền riêng tư và bảo mật thông tin.

Ngoài việc bảo vệ bảo mật, các cập nhật định kỳ cũng thường đi kèm với các cải tiến về hiệu suất và sự ổn định của hệ thống. Điều này giúp tăng cường khả năng hoạt động của các ứng dụng và thiết bị, làm giảm khả năng gặp phải các lỗi và trục trặc không mong muốn.

IV. Cơ chế bảo vệ dữ liệu

4.1. Giới thiệu về BitLocker, công cụ mã hóa ổ đĩa của Windows

Trong bối cảnh công nghệ thông tin ngày càng phát triển, việc bảo vệ dữ liệu cá nhân và doanh nghiệp trở nên vô cùng quan trọng. Để đối phó với các mối đe dọa về bảo mật, Microsoft đã phát triển BitLocker - một công cụ mã hóa ổ đĩa mạnh mẽ tích hợp sẵn trong hệ điều hành Windows. BitLocker được giới thiệu lần đầu trong Windows Vista và hiện nay đã trở thành một phần không thể thiếu của các phiên bản Windows sau này như Windows 7, 8, 10 và 11.



Hình 6: BitLocker

BitLocker giúp bảo vệ dữ liệu bằng cách mã hóa toàn bộ ổ đĩa, đảm bảo rằng chỉ những người có quyền truy cập hợp lệ mới có thể đọc được thông tin lưu trữ trên đó. Công cụ này sử dụng thuật toán mã hóa AES (Advanced Encryption Standard) với các khóa mã hóa 128-bit hoặc 256-bit, mang lại mức độ bảo mật cao.

4.2. Cách hoạt động và lợi ích của việc sử dụng BitLocker

**Cách thức hoạt động của BitLocker:*

Quá Trình Mã Hóa: BitLocker sử dụng thuật toán AES (Advanced Encryption Standard) với độ dài khóa 128-bit hoặc 256-bit để mã hóa dữ liệu trên ổ đĩa. Khi kích hoạt, BitLocker mã hóa toàn bộ ổ đĩa hoặc chỉ không gian sử dụng. Mã hóa toàn bộ ổ đĩa bảo vệ tất cả các tệp tin, trong khi mã hóa không gian sử dụng chỉ bảo vệ các tệp tin hiện có.

Sử Dụng TPM (Trusted Platform Module): TPM là một chip bảo mật tích hợp trên bo mạch chủ của máy tính, giúp lưu trữ khóa mã hóa an toàn. TPM đảm bảo rằng chỉ hệ thống đáng tin cậy mới có thể truy cập khóa mã hóa, ngăn chặn các cuộc tấn công vật lý và phần mềm. Nếu không có TPM, BitLocker có thể sử dụng

mật khẩu hoặc USB chứa khóa mã hóa.

Quá Trình Khởi Động An Toàn: BitLocker kiểm tra tính toàn vẹn của hệ thống trước khi khởi động hệ điều hành. Nếu không phát hiện thay đổi, TPM sẽ cung cấp khóa mã hóa để mở khóa ổ đĩa. Dữ liệu được giải mã khi truy cập và mã hóa lại khi lưu trữ, đảm bảo bảo mật mà không ảnh hưởng đến hiệu suất hệ thống.

Quản Lý Khóa: BitLocker cung cấp khóa khôi phục để truy cập dữ liệu trong trường hợp quên mật khẩu hoặc thay đổi phần cứng. Khóa khôi phục có thể được lưu trữ trên tài khoản Microsoft, USB, in ra giấy, hoặc lưu vào tệp tin. Khóa mã hóa được lưu trữ an toàn trong TPM hoặc USB, giúp tự động mã hóa và giải mã dữ liệu khi cần.

Quá Trình Giải Mã: Người dùng có thể tắt BitLocker bất kỳ lúc nào, và hệ thống sẽ bắt đầu giải mã toàn bộ dữ liệu trên ổ đĩa, quá trình này mất thời gian tương tự như khi mã hóa.

**Lợi ích của việc sử dụng BitLocker:*

Bảo Vệ Dữ Liệu: BitLocker mã hóa dữ liệu trên ổ cứng máy tính, ngăn chặn truy cập trái phép khi thiết bị bị mất hoặc đánh cắp, đảm bảo thông tin nhạy cảm luôn được an toàn.

Tăng Cường Bảo Mật: Công cụ này bảo vệ dữ liệu khỏi các cuộc tấn công bằng phần mềm độc hại và phần cứng không đáng tin cậy. Sử dụng TPM (Trusted Platform Module) để lưu trữ khóa mã hóa an toàn, ngăn chặn các cuộc tấn công vật lý và phần mềm.

Tăng tính linh Hoạt: Phần mềm có thể được sử dụng trên nhiều thiết bị khác nhau, bao gồm cả ổ đĩa di động, cho phép bảo vệ dữ liệu trên cả máy tính cá nhân và thiết bị lưu trữ di động.

Dễ Dàng Sử Dụng: Với giao diện thân thiện, người dùng có thể dễ dàng bật/tắt mã hóa và quản lý khóa mã hóa. Các tùy chọn lưu trữ khóa khôi phục đa dạng giúp quản lý và truy cập dữ liệu thuận tiện.

4.3. Phương pháp sao lưu và phục hồi dữ liệu trên Windows

Sao lưu và khôi phục dữ liệu trên Windows là một biện pháp quan trọng giúp bảo vệ thông tin và đảm bảo tính sẵn sàng trong các tình huống khẩn cấp. Dưới đây là một vài công cụ Windows cung cấp để người dùng có thể sử dụng:

Windows Backup and Restore: Phương pháp cơ bản cho phép sao lưu các

tệp và thư mục quan trọng trên máy tính. Có thể thiết lập lịch trình sao lưu tự động để đảm bảo dữ liệu luôn được cập nhật và an toàn.

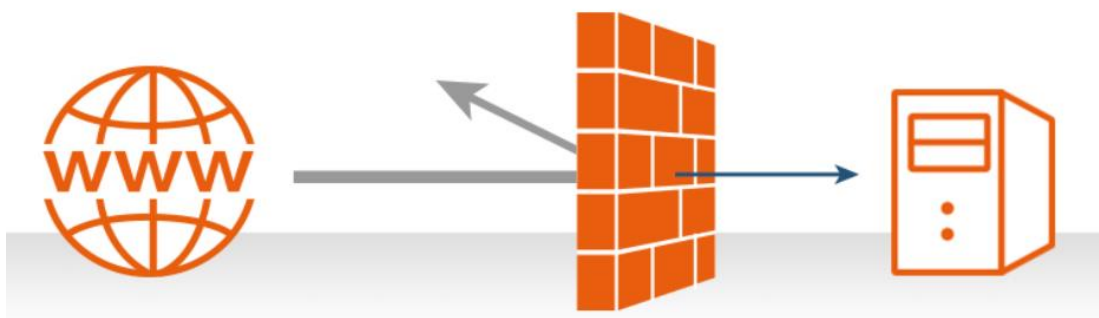
File History: Tự động sao lưu các phiên bản trước của các tệp trong các thư mục quan trọng như Documents, Pictures, và Desktop. Cho phép người dùng khôi phục lại các phiên bản tệp trước đó một cách dễ dàng từ các bản sao lưu.

OneDrive: Dịch vụ lưu trữ đám mây của Microsoft, cho phép người dùng lưu trữ và đồng bộ hóa các tệp từ nhiều thiết bị. Tệp được lưu trữ trên OneDrive có thể truy cập từ bất kỳ đâu có kết nối Internet.

V. Cơ chế bảo vệ tường lửa và mạng

5.1. Giới thiệu về tường lửa của Windows(Windows Firewall)

Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, hoạt động bằng cách sử dụng các quy tắc để kiểm soát lưu lượng truy cập vào và ra khỏi hệ thống. Nó hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn, kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Chỉ có những lưu lượng truy cập phù hợp với chính sách được định nghĩa trong tường lửa mới được phép truy cập vào mạng, mọi lưu lượng truy cập không phù hợp sẽ bị từ chối.



Hình 7: Tường lửa

...

Firewall có thể được phân thành hai loại chính:

Firewall cứng (Hardware Firewall): là một thiết bị phần cứng được tích hợp trong hệ thống mạng, như router, switch, hoặc gateway. Nó hoạt động dựa trên các quy tắc cấu hình trước để kiểm soát và bảo vệ mạng máy tính. Firewall cứng có hiệu suất cao và bảo mật mạnh mẽ, phù hợp cho các môi trường mạng doanh nghiệp và tổ chức lớn.

Firewall mềm (Software Firewall): là phần mềm được cài đặt và chạy trên hệ điều hành máy tính cá nhân hoặc máy chủ. Nó cung cấp bảo vệ mạng cho từng thiết bị cụ thể và thường đi kèm với hệ điều hành như Windows, macOS, Linux. Firewall mềm có thể cấu hình và quản lý dễ dàng từ máy tính, nhưng hiệu suất thường thấp hơn so với firewall cứng khi xử lý lưu lượng mạng lớn.

5.2. Cách tường lửa Windows giúp bảo vệ hệ thống

Tường lửa Windows bảo vệ hệ thống của người dùng thông qua một loạt các cơ chế quan trọng:

Chặn kết nối không mong muốn: Tường lửa Windows theo dõi tất cả các kết nối mạng đến và đi từ máy tính của người dùng sau đó quyết định cho phép hay chặn các kết nối này dựa trên một loạt các quy tắc đã được định rõ. Quy tắc này có thể được tự động xác định bởi hệ thống hoặc do người dùng đặt.

Quản lý truy cập ứng dụng: Tường lửa Windows kiểm soát ứng dụng nào có thể gửi và nhận dữ liệu qua mạng. Nếu một ứng dụng không được phép truy cập mạng, tường lửa sẽ chặn nó, ngăn chặn việc truyền thông tin cá nhân hoặc phát tán phần mềm độc hại.

Bảo vệ từ các cuộc tấn công từ bên ngoài: Tường lửa ngăn chặn các cuộc tấn công từ bên ngoài như việc khai thác các lỗ hổng bảo mật, từ chối dịch vụ và các cuộc tấn công khác đang cố gắng truy cập máy tính của người dùng mà không có sự cho phép.

Ngăn chặn việc phát tán phần mềm độc hại: Nếu máy tính của người dùng nhiễm phần mềm độc hại, tường lửa có thể ngăn chặn nó truy cập mạng và phát tán đến các máy tính khác trong mạng.

Hỗ trợ phát hiện xâm nhập: Mặc dù không phải là một hệ thống phát hiện xâm nhập đầy đủ, tường lửa Windows có các tính năng cơ bản của hệ thống đó, giúp phát hiện các mẫu truy cập bất thường hoặc đáng ngờ.

5.3. Các cơ chế bảo vệ mạng khác:

Để bảo vệ mạng, Windows sử dụng một loạt các cơ chế bảo vệ khác bên cạnh tường lửa. Một số các cơ chế bảo vệ khác của Windows:

Cảnh báo an ninh mạng (Network Security Monitoring - NSM): Giám sát liên tục hoạt động mạng để phát hiện các hành vi không bình thường, cung cấp cảnh báo sớm về các mối đe dọa tiềm ẩn và các cuộc tấn công.

Cài đặt quyền truy cập mạng (Network Access Control - NAC): Xác định và kiểm soát quyền truy cập vào mạng dựa trên các chính sách an ninh, bao gồm xác thực người dùng, quản lý thiết bị và áp dụng các hạn chế truy cập để đảm bảo tính bảo mật mạng.

Windows Security: là trung tâm quản lý bảo mật tích hợp trong hệ điều hành Windows. Nó cung cấp các công cụ như Windows Defender Antivirus, Firewall & Network Protection, Device Security và cấu hình bảo mật khác để ngăn chặn virus, phần mềm độc hại và các cuộc tấn công mạng.

Windows Update: là công cụ cho phép cập nhật các bản vá bảo mật, cải tiến và tính năng mới cho hệ điều hành Windows. Nó tự động tải và cài đặt các cập nhật từ Microsoft, giúp duy trì tính bảo mật và hiệu suất của hệ thống.

VI. Thực nghiệm

6.1. Cơ chế kiểm soát truy cập

Mục tiêu

Mục tiêu của bài này là làm quen với các tính năng kiểm soát truy cập có sẵn trong các hệ thống dựa trên Microsoft Windows.

Bối cảnh

Kiểm soát truy cập (Access control) đề cập đến khả năng của người dùng truy cập vào một đối tượng cụ thể và có thể sửa đổi nó. Trong ngữ cảnh của hệ điều hành, kiểm soát truy cập đề cập đến khả năng của một người sử dụng để đọc, viết hoặc

thực thi một tập tin hoặc thư mục nhất định. Trong bài này, chúng ta sẽ nghiên cứu khung (framework) điều khiển truy cập cho các nền tảng dựa trên Microsoft Windows.

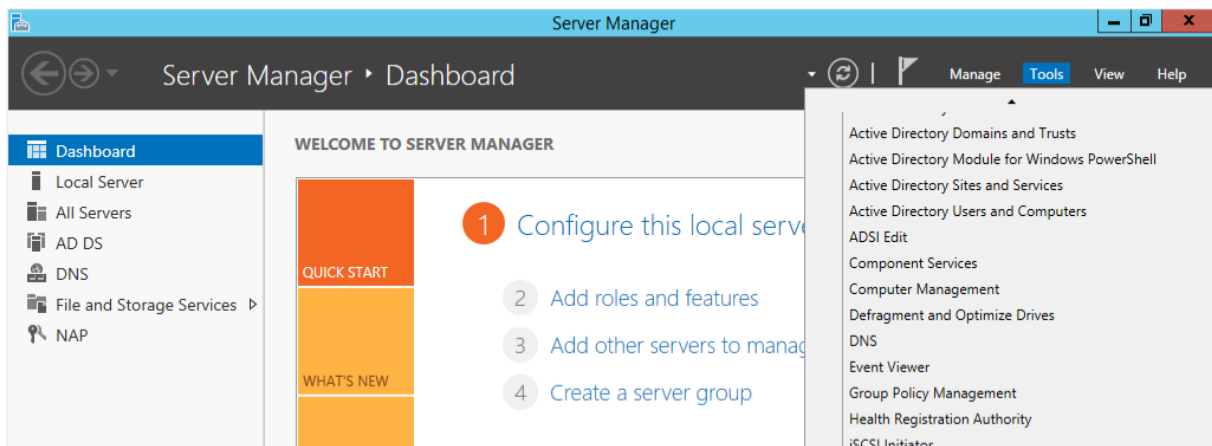
Tài nguyên yêu cầu

Một PC hoặc máy ảo với Microsoft Windows 2000/XP/Vista hay tương tự.

Kiểm soát truy cập

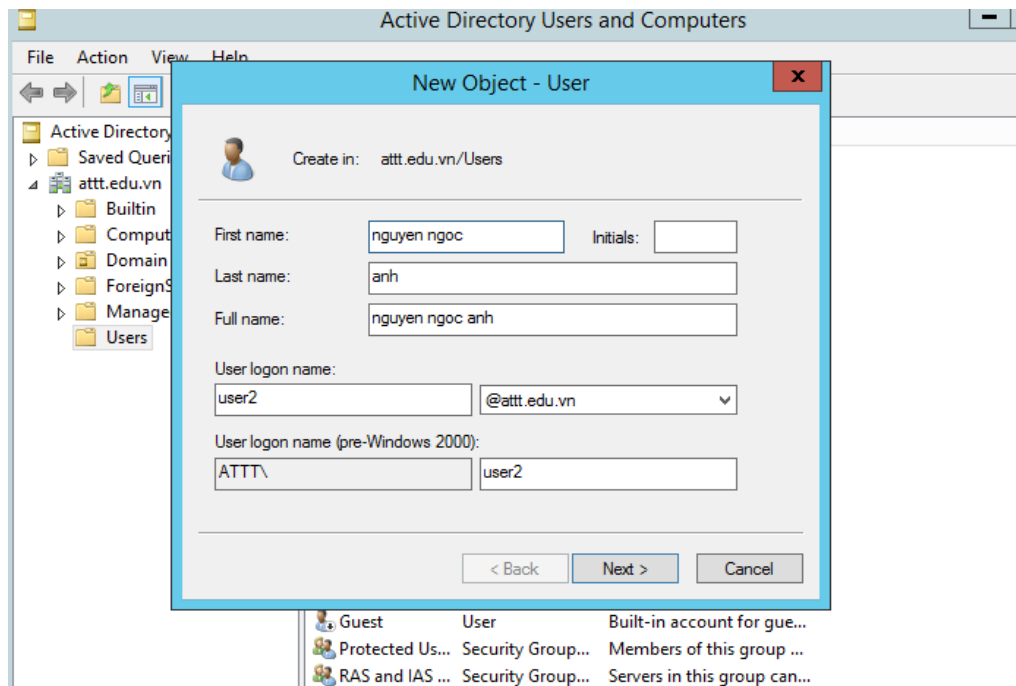
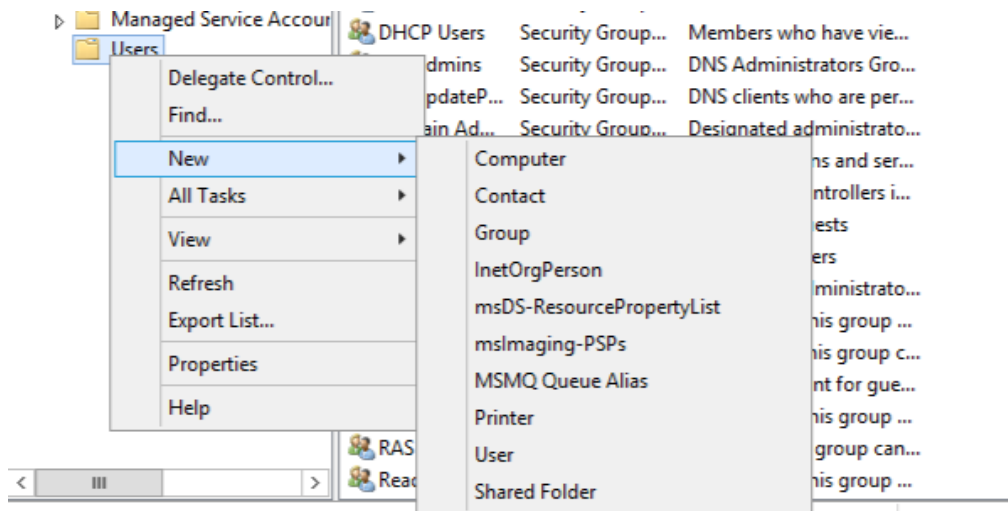
Bài 1: Thêm user vào hệ thống

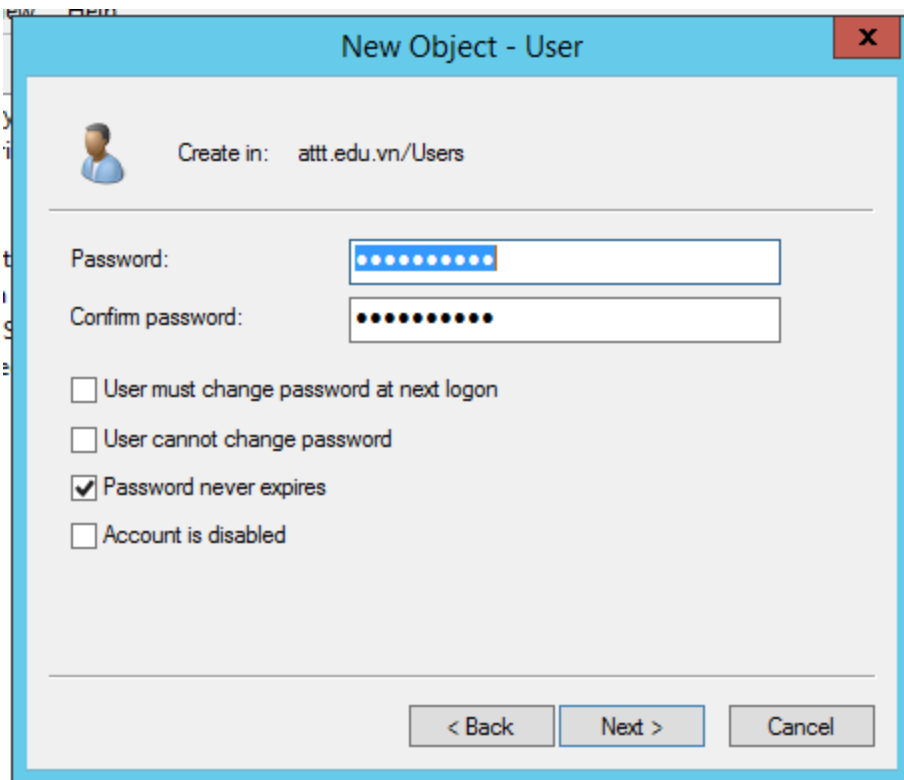
1. Log in vào tài khoản của Admin trên Windows Server 2012.
2. Tại Server Manager nhấn vào Tools -> Active Directory Users and Computers .



Hình 8: Server Manager

3. Nhấn chuột phải vào Users -> New -> User -> Nhập thông tin tài khoản -> Set password.



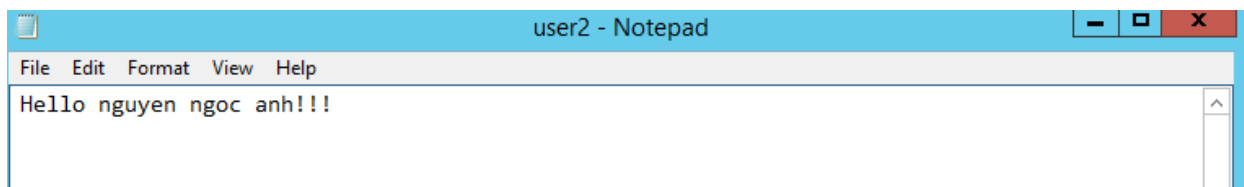


Hình 9: Cách add user vào hệ thống

4. Nhấn Finish.

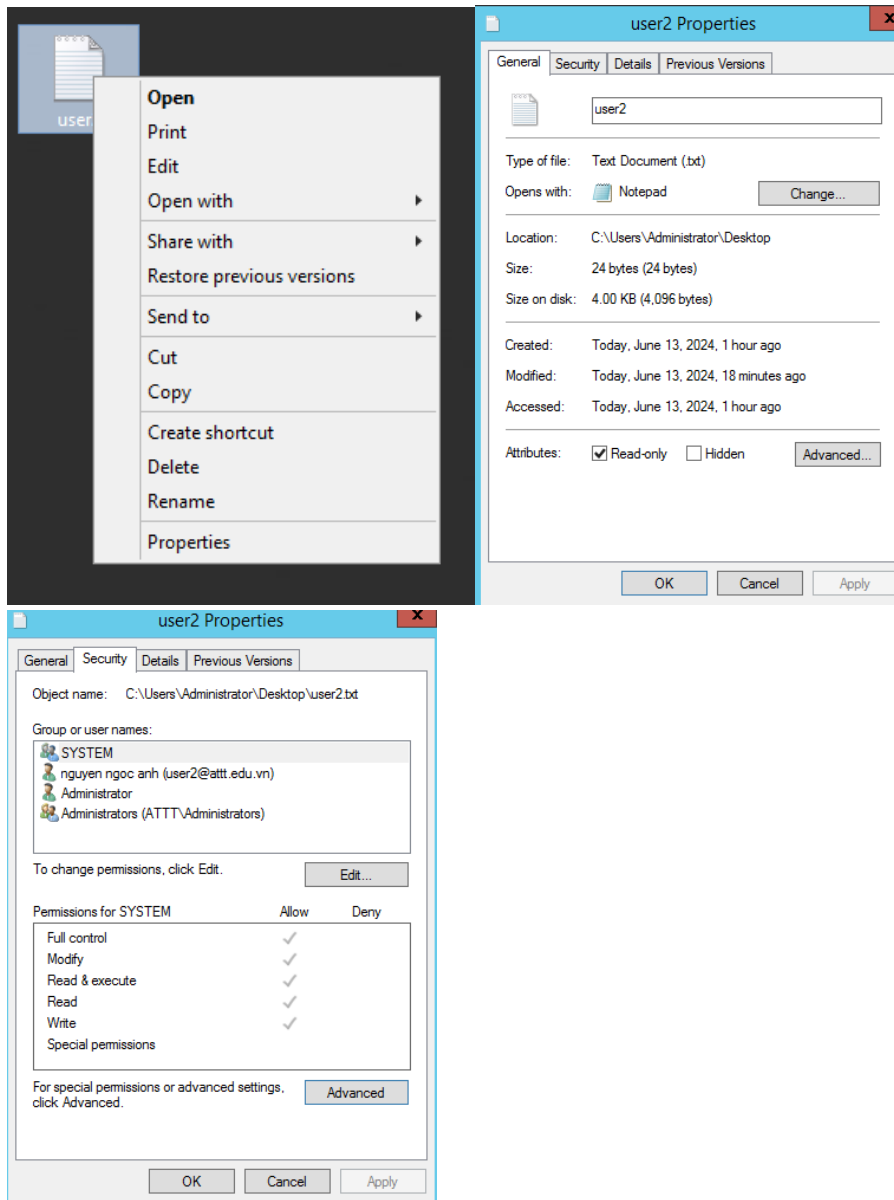
Bài 2: Tìm hiểu tác dụng của các thuộc tính Read-Only và Hidden của một file

1. Log in vào tài khoản của Admin trên Windows Server 2012.
2. Mở ứng dụng *Notepad* để tạo 1 file văn bản với tên **user2.txt**.



Hình 10: Tạo file .text bằng Notepad

3. Chuột phải vào **user2.txt** -> chọn **Properties** -> **Read-only** -> **Security** -> **Advanced** -> **Add** -> **Select a principal** -> Gõ tên người dùng -> **Check Names** xem có tồn tại người dùng này không -> **OK** -> **Apply**.



Advanced Security Settings for user2

Name: C:\Users\Administrator\Desktop\user2.txt

Owner: Administrators (ATT\Administrators) [Change](#)

Permissions | Share | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

| Type | Principal | Access | Inherited from |
|-------|-------------------------------------|----------------|-------------------------|
| Allow | nguyen ngoc anh (user2@att.edu.vn) | Read & execute | None |
| Allow | SYSTEM | Full control | C:\Users\Administrator\ |
| Allow | Administrators (ATT\Administrators) | Full control | C:\Users\Administrator\ |
| Allow | Administrator | Full control | C:\Users\Administrator\ |

[Add](#) [Remove](#) [View](#)

[Disable inheritance](#)

[OK](#) [Cancel](#) [Apply](#)

Permission Entry for user2

Principal: [Select a principal](#)

Type: [Allow](#)

Basic permissions: [Show advanced permissions](#)

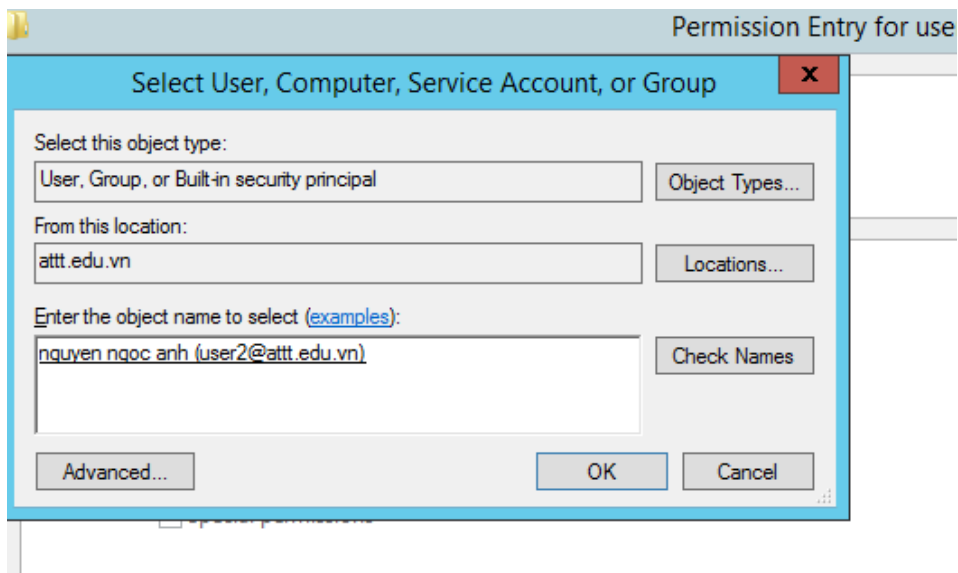
☐ Full control
☐ Modify
☒ Read & execute
☒ Read
☐ Write
☐ Special permissions

[Clear all](#)

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Add a condition

[OK](#) [Cancel](#)

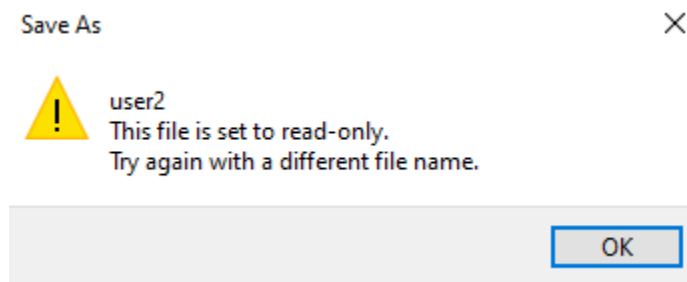


Hình 11: Cách share, set Read-Only cho folder và phân quyền cho user

4. Đăng nhập vào user2 tại Windows 10 và mở lại file (Windows + R -> [\\192.168.1.1](http://192.168.1.1) -> Users -> Administrator -> Desktop (Mình lưu file nó ở chỗ này nên mới có đường dẫn này) -> user2.txt): chỉnh sửa rồi thử lưu.

1) Điều gì xảy ra? Tại sao?

Thông báo lỗi là không thể thay đổi file chỉ được đọc. Vì ta đã cài đặt cho file với quyền Read-only bằng account Admin nên nếu muốn lưu thay đổi cần đổi lại thuộc tính và cấp thêm quyền *Modify* cho user2.



Hình 12: Thông báo người dùng user2 không thể chỉnh sửa file

5. Tại tài khoản user2 (Điều kiện: user2 phải có quyền **Full control**) đánh dấu **Hidden -> OK**

1) Bây giờ bạn có thấy file không? **Không**

2) Nếu bạn không thấy file, hãy thử tìm cách để hiện file ẩn.

Mở File Explorer trên máy tính, chọn View

Tại mục View, chọn Show hidden files, folders, and drives

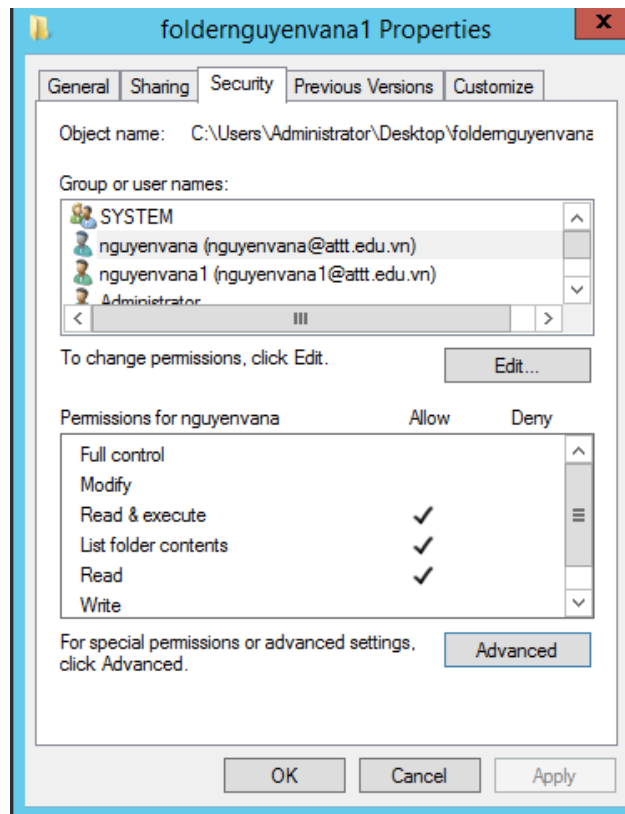
Bài 3: Hiểu cơ chế kiểm soát truy cập của MS Windows

1. Log in vào tài khoản của Admin trên Windows Sever 2012
2. Tạo thêm người dùng trong hệ thống. Tên người dùng sẽ là *nguyenvana* (Tham Bài 1).
3. Tại màn hình Desktop tạo 1 thư mục tên là *foldernguyenvana1* và Share thư mục này với *nguyenvana* và *nguyenvana1*
4. Chọn thư mục vừa tạo và mở *Properties* của nó.
5. Chọn tab *Security* và nhấn vào *Edit*.
6. Nhấn nút *Add* và thêm user *nguyenvana*. Nhớ nhấn *Check Names* trước khi nhấn OK.
7. Chọn user *nguyenvana* trong cửa sổ *Permissions*. Quyền gì hiện được gán cho user này?

Read & execute

List folder contents

Read



Hình 13: Permissions mặc định khi thêm user có quyền với file hoặc folder

8. Đánh dấu quyền *List folder contents* vào cột *Deny*. Nhấn OK và chấp nhận các thay đổi.
9. Log in vào tài khoản *nguyenvana1* trên Windows 10
10. Mở Notepad và tạo một file văn bản
11. Thêm nội dung và lưu nó vào thư mục *foldernguyenvana1* với tên là *nguyenvana1.txt*. Kết quả có lưu được không? Tại sao?

Không thể lưu. Bởi vì user *nguyenvana1* chỉ có 3 quyền mặc định: Read, Read & execute, List folder contents.

12. Log off khỏi tài khoản *nguyenvana1* và log in *nguyenvana*.
13. Mở thư mục *foldernguyenvana1*. Điều gì sẽ xảy ra khi bạn truy cập vào thư mục và tại sao?

Không tìm thấy thư mục *foldernguyenvana1*.

Vì admin đã setup từ chối việc liệt kê dữ liệu trong folder đồng nghĩa với việc bị từ chối truy cập folder đó.

6.2. Bảo vệ tài khoản

Mục tiêu

Mục tiêu của bài này là làm quen với các tính năng bảo vệ tài khoản có sẵn trên Microsoft Windows.

Để minh họa các cơ chế bảo vệ tài khoản trong Windows, ta sẽ thực hiện các bước sau:

1. Sử dụng mật khẩu mạnh:

- Mở **Settings > Accounts > Sign-in options**.
- Nhấp vào **Change PIN** dưới **PIN**.
- Nhấp vào **Change password** dưới **Password**.
- Tạo mật khẩu mạnh bao gồm ít nhất 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- Xác nhận mật khẩu mới.

2. Bật xác thực hai yếu tố (2FA):

- Nhấp vào **Manage two-factor authentication** dưới **Two-factor authentication**.
- Chọn phương thức 2FA mong muốn, ví dụ: ứng dụng xác thực hoặc số điện thoại.
- Làm theo hướng dẫn để thiết lập 2FA.

3. Sử dụng Windows Hello:

- Mở **Settings > Accounts > Sign-in options**.
- Nhấp vào **Set up Windows Hello** dưới **Face recognition** hoặc **Set up Windows Hello** dưới **Fingerprint**.
- Làm theo hướng dẫn để thiết lập Windows Hello.

4. Khóa tài khoản khi không sử dụng:

- Mở **Settings > Accounts > Sign-in options**.
- Di chuyển thanh trượt dưới **Dynamic lock** sang vị trí **On**.
- Chọn thiết bị bạn muốn sử dụng để khóa tài khoản.

5. Tạo tài khoản người dùng hạn chế:

- Mở **Settings > Accounts > Family & other users**.
- Nhấp vào **Add a family member**.
- Chọn **I don't have this person's email address**.
- Nhấp vào **Add a child without an account**.
- Tạo tên và mật khẩu cho tài khoản người dùng hạn chế.

6.3. Tường lửa

Mục tiêu

Mục tiêu của bài này là làm quen với các tính năng chặn IP, chặn kết nối Internet các ứng dụng hay chương trình nào đó trong các hệ thống dựa trên Microsoft Windows.

Bối cảnh

Tường lửa (Firewall) là một hệ thống bảo mật mạng giám sát và kiểm soát lưu lượng mạng đến và đi. Tường lửa thiết lập một rào cản giữa một mạng nội bộ đáng tin cậy và mạng bên ngoài không tin cậy, chẳng hạn như Internet. Trong bài này, chúng ta sẽ nghiên cứu khả năng Allow/Block các Rules trong *Inbound Rules* và *Outbound Rules* của hệ thống Firewall cho các nền tảng dựa trên Microsoft Windows.

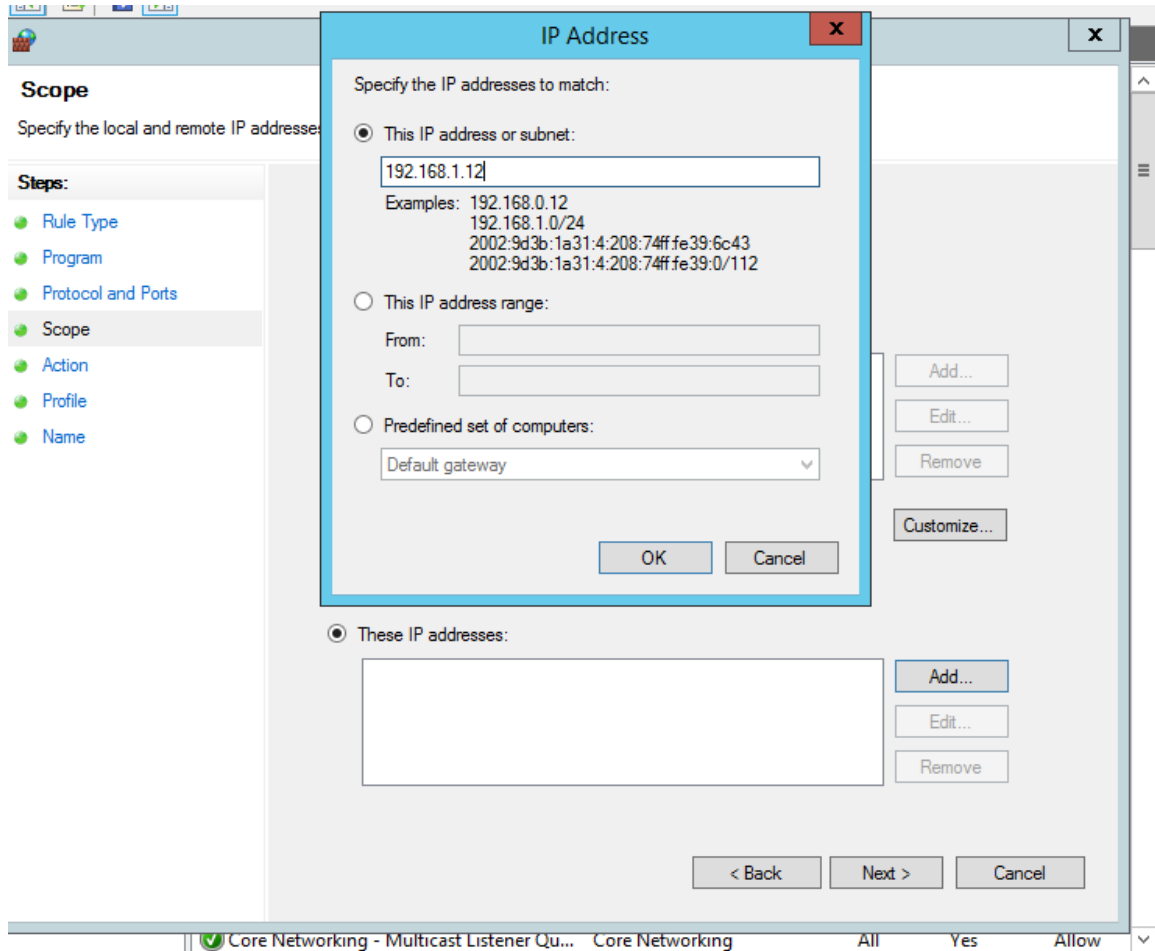
Tài nguyên yêu cầu

Một PC hoặc máy ảo với Microsoft Windows 2000/XP/Vista hay tương tự.

Bài 1: Tìm hiểu về chức năng Allow/Block IP client kết nối tới Server với Inbound Rules.

1. Log in vào tài khoản admin
2. Chọn Start -> Search -> Windows Firewall with Advanced Security
3. Chọn Inbound Rules -> New Rule -> Custom -> Next -> Next -> Next

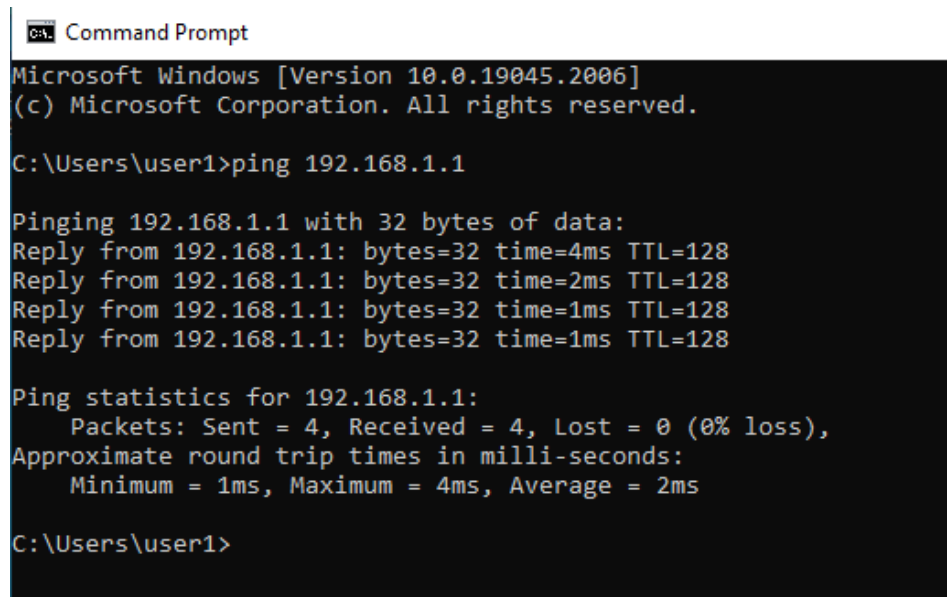
4. Tại cửa sổ *Scope* , có 2 chế độ áp dụng Rule cho IP (IP local và IP remote: mỗi chế độ thì lại có 2 option(*Any IP address* và *These IP address*)) mình muốn chặn IP remote từ xa thì tại chế độ *Which remote IP addresses does this rule apply to?* chọn *These IP address* -> Add -> 192.168.1.12 (IP của máy khách) -> OK -> Next



Hình 14: Gán địa chỉ IP tại Scope

5. Tại *Action* Chọn *Allow the connection* -> Next -> Next
6. Cuối cùng đặt tên cho Rule là *Allow IP 192.168.1.12* rồi bấm *Finish*.
7. Log in vào máy có IP là 192.168.1.12 (IP của máy khách) với tài khoản user là *user1* (đã tạo trước đó và thêm vào hệ thống)
8. Chọn *Start* -> *Search* -> Gõ *Command Prompt* và ping thử tới Server(IP: 192.168.1.1) với câu lệnh sau:
- ping 192.168.1.1*
- Có kết nối được tới Server không?

Kết quả: Ping thành công từ máy khách (192.168.1.12) tới máy Server (192.168.1.1)



```

C:\> Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user1>ping 192.168.1.1

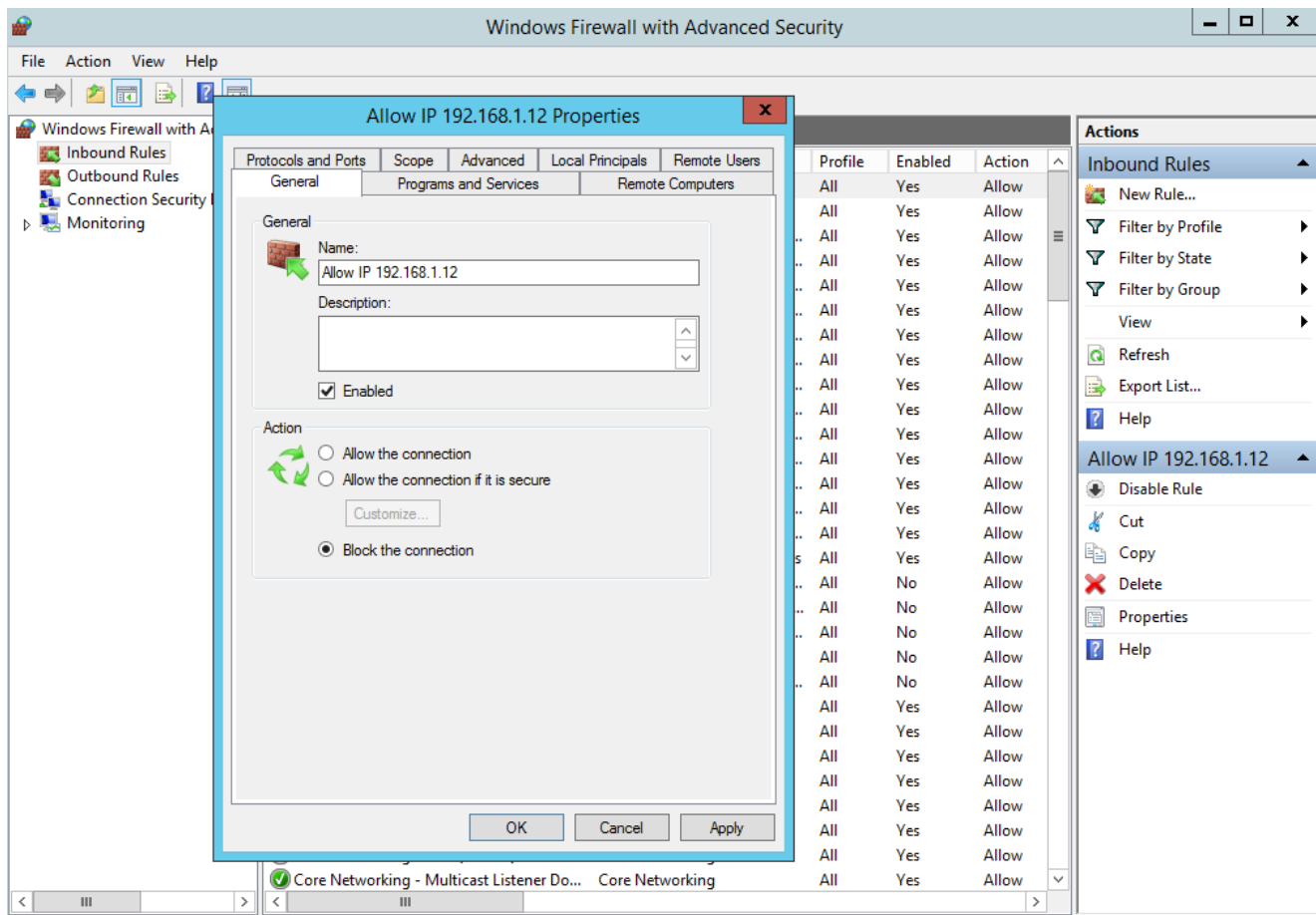
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Users\user1>
```

Hình 15: Ping thành công từ máy Client đến máy Server khi Server cho phép connect

9. Quay lại máy Server với tài khoản admin
10. Bấm chuột phải vào Rule với tên *Allow IP 192.168.1.12* rồi chọn Properties
-> Block the connection -> Apply -> OK



Hình 16: Thay đổi Rule bằng cách vào Properties của Rule đó

11. Quay trở lại với máy khách (192.168.1.12) với tài khoản *user1*
12. Ping lại tới Server . Server đã chặn kết nối thành công chưa ?

Kết quả: Đã bị chặn kết nối tới Server

```

C:\> Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Users\user1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

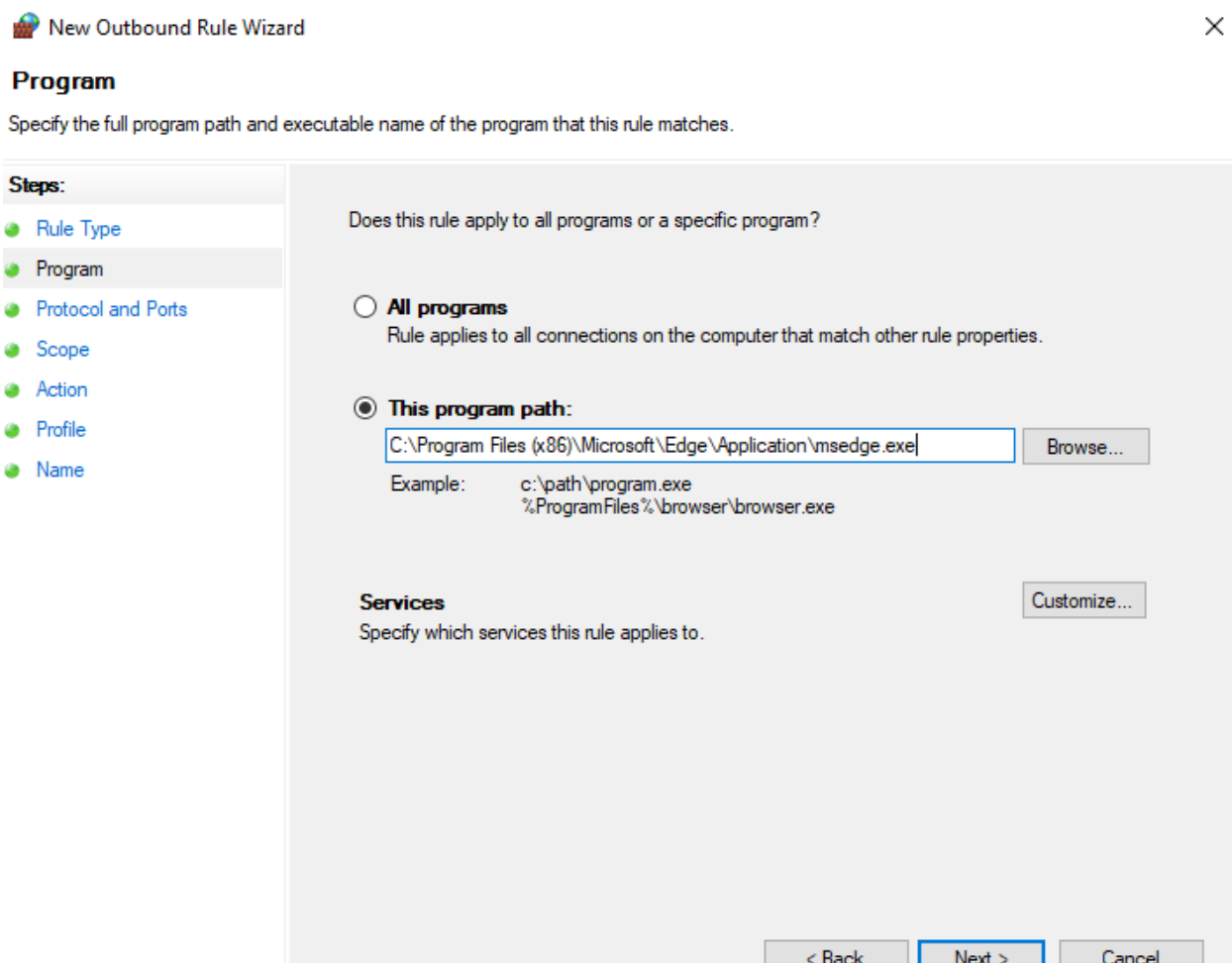
C:\Users\user1>_

```

Hình 17: Ping thất bại từ máy Client đến Server khi Server chặn connection

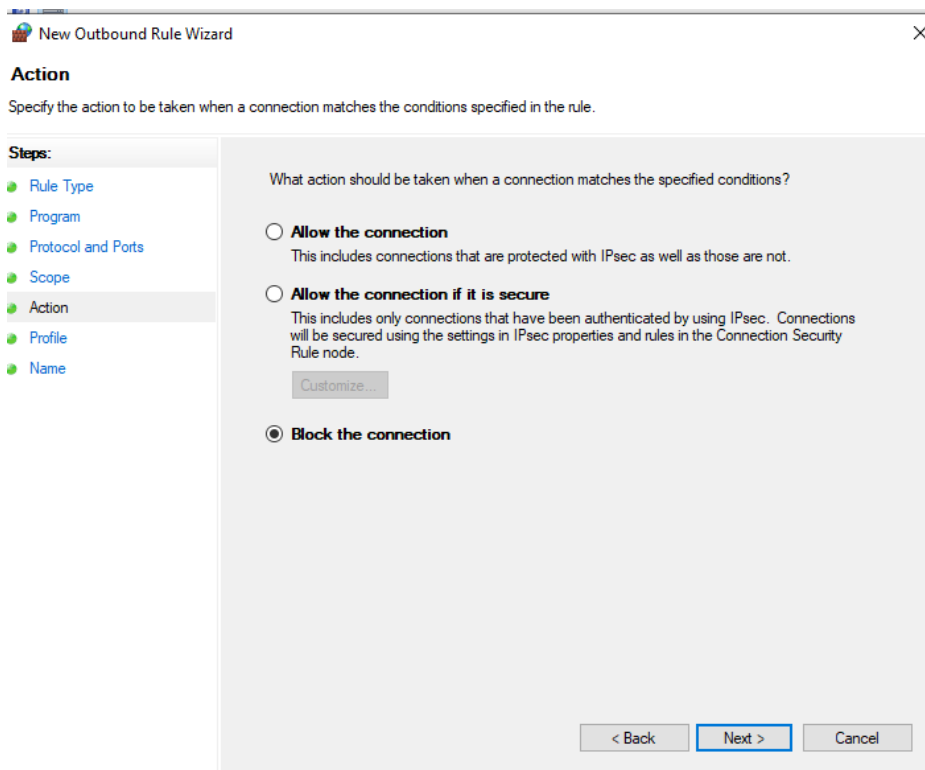
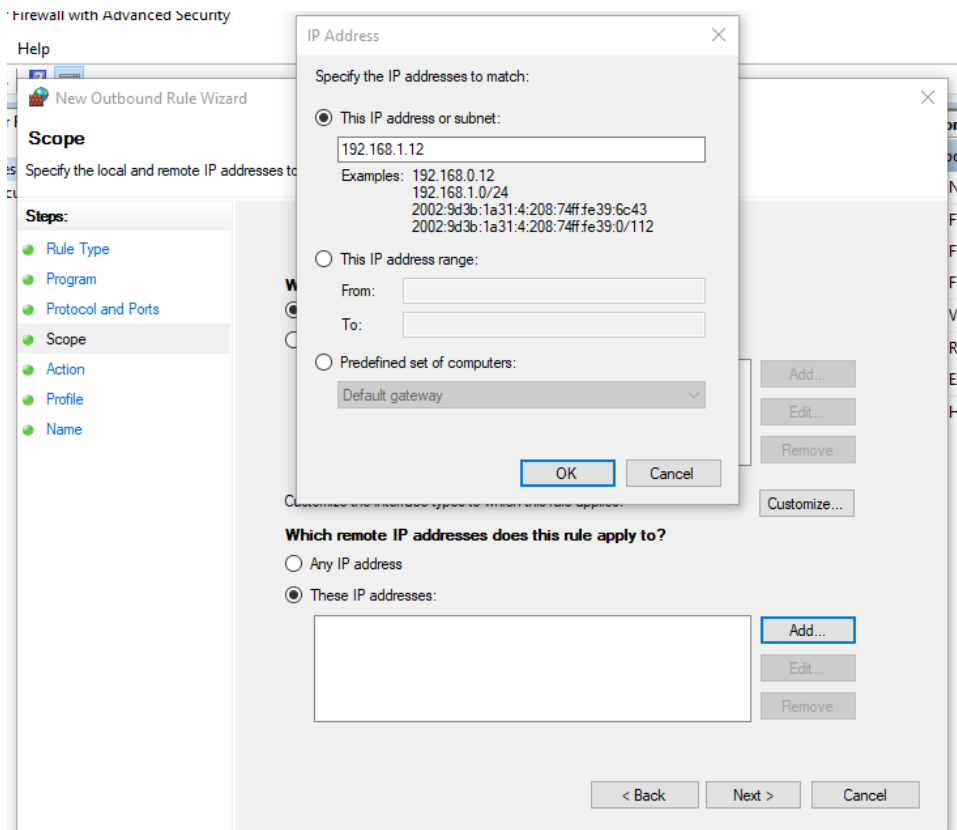
Bài 2: Tìm hiểu chức năng chặn IP client truy cập Internet của một ứng dụng hay program nào đó với Outbound Rules.

1. Log in vào tài khoản admin tại máy Server
2. Chọn Start -> Search -> Windows Firewall with Advanced Security
3. Chọn Outbound Rules -> New Rule -> Custom -> Next -> This program path rồi dán đường dẫn ứng dụng nào đó cần truy cập Internet



Hình 18: Dán đường dẫn của một ứng dụng nào đó tại Program của Outbound Rules

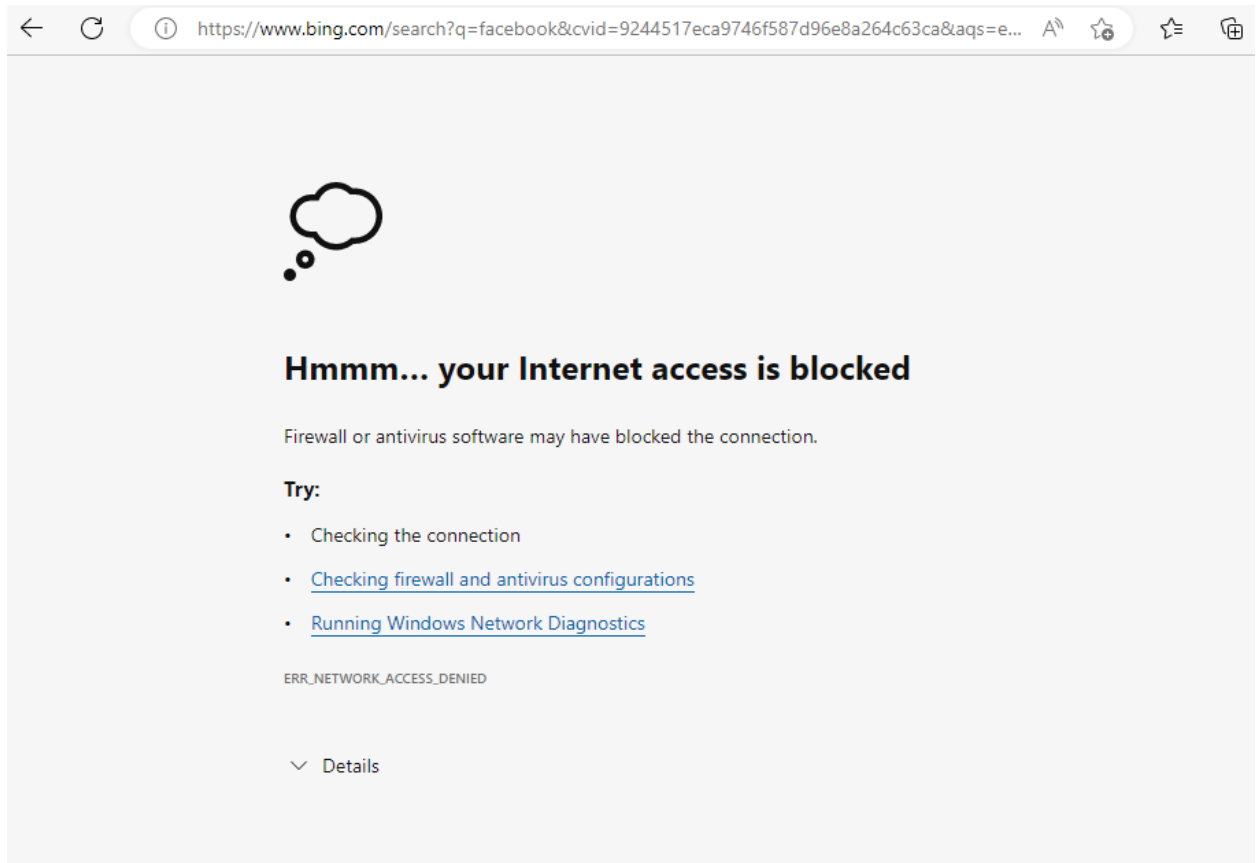
4. Bấm Next cho đến Scope bấm These IP addresses (tại Which remote IP addresses does this rule apply to) -> Add -> 192.168.1.12 (IP máy client) -> OK -> Next -> Block the connection -> Next



Hình 19: Block connect Internet của một ứng dụng MS Edge mà máy client đang sử dụng

5. Cuối cùng đặt *Name* cho Rule là *Block connect Internet(Edge) 192.168.1.12*.
6. Log in vào máy client (IP: 192.168.1.12) với tài khoản *user1*
7. Mở *Microsoft Edge* và gõ Facebook. Có truy cập được Internet không?

Kết quả: Không thể truy cập được Internet tại ứng dụng *Edge*



Hình 20: Máy Client (192.168.1.12) đã bị chặn truy cập Internet tại MS Edge

VII. Kết luận

7.1. Tầm quan trọng của việc hiểu và áp dụng đúng các cơ chế bảo vệ của Windows

Hiểu và áp dụng đúng các cơ chế bảo vệ của Windows rất quan trọng vì các lý do sau đây:

- Bảo vệ dữ liệu:

Dữ liệu là một trong những tài sản quý giá nhất mà mỗi người dùng hoặc tổ chức sở hữu. Dữ liệu có thể bao gồm thông tin cá nhân, thông tin tài chính, dữ liệu khách hàng, tài liệu quan trọng và nhiều hơn nữa. Các cơ chế bảo vệ của Windows giúp bảo vệ những dữ liệu này khỏi bị mất hoặc bị đánh cắp.

- Bảo vệ hệ thống:

Các hệ thống máy tính là mục tiêu chính của nhiều loại tấn công mạng. Các cơ chế bảo vệ của Windows giúp bảo vệ hệ thống của người dùng khỏi các loại tấn công như mã độc, ransomware, và các cuộc tấn công khai thác lỗ hổng.

- Duy trì hiệu suất:

Một hệ thống bị nhiễm mã độc hoặc đang bị tấn công có thể hoạt động chậm và không ổn định. Bằng cách giữ cho hệ thống an toàn, các cơ chế bảo vệ của Windows giúp duy trì hiệu suất máy tính của người dùng.

- Tăng cường niềm tin:

Cho dù người sử dụng là một cá nhân hay một doanh nghiệp, việc giữ an toàn cho dữ liệu và hệ thống sẽ tăng cường niềm tin từ người dùng và khách hàng.

Cuối cùng, việc hiểu các cơ chế bảo vệ của Windows không chỉ giúp người sử dụng bảo vệ máy tính của mình mà còn giúp phát triển một tư duy bảo mật toàn diện, giúp người dùng an toàn khi sử dụng công nghệ trong cuộc sống hàng ngày.

7.2. Khuyến nghị về việc tiếp tục cập nhật kiến thức về an ninh mạng và bảo vệ hệ thống

An ninh mạng và bảo vệ hệ thống là một lĩnh vực liên tục phát triển, với các mối đe dọa mới xuất hiện và các cách phòng ngừa mới được phát triển.

Một số khuyến nghị để giúp người dùng kiến thức về an ninh mạng và bảo vệ hệ thống:

- Đọc các bài viết và blog:

Có rất nhiều nguồn thông tin trực tuyến về an ninh mạng và bảo vệ hệ thống, từ các blog chuyên sâu đến các bài viết trên các trang tin tức công nghệ uy tín. Đọc các nguồn này có thể giúp người dùng nắm bắt được xu hướng mới và hiểu rõ hơn về các mối đe dọa tiềm ẩn.

- Tham gia các khóa học trực tuyến:

Có nhiều khóa học trực tuyến về an ninh mạng và bảo vệ hệ thống, từ những khóa học miễn phí đến những khóa học có phí với chứng chỉ chuyên nghiệp. Các khóa học này có thể cung cấp cho người dùng một hiểu biết sâu sắc về lĩnh vực này.

- Tham gia các diễn đàn và cộng đồng trực tuyến:

Có nhiều diễn đàn và cộng đồng trực tuyến về an ninh mạng và bảo vệ hệ thống, nơi mà người sử dụng có thể hỏi câu hỏi, chia sẻ kiến thức, và tìm hiểu từ người khác.

- Cập nhật thường xuyên hệ thống và phần mềm bảo mật:

Đảm bảo rằng hệ thống và phần mềm bảo mật của mình được cập nhật thường xuyên là một cách tốt để tự bảo vệ khỏi các mối đe dọa mới nhất.

- Thực hành các thói quen bảo mật tốt:

Việc học về an ninh mạng và bảo vệ hệ thống không chỉ là về việc nắm bắt thông tin, mà còn về việc áp dụng những gì đã học vào thực tế. Điều này có thể bao gồm việc thiết lập mật khẩu mạnh, không mở các tệp hoặc liên kết đáng ngờ, và duy trì các bản sao lưu dữ liệu thường xuyên.

Bằng cách tiếp tục học hỏi và cập nhật kiến thức về an ninh mạng và bảo vệ hệ thống, mỗi cá nhân không chỉ giúp bảo vệ mình và dữ liệu của mình, mà còn giúp củng cố vào một mạng lưới thông tin an toàn hơn cho tất cả mọi người.

CÀI ĐẶT MÔI TRƯỜNG MÁY ẢO

1. Cài đặt công cụ Virtual Box hoặc VMWare, máy ảo Windows 10 và Windows Server 2012

Bước 1: Cài đặt VirtualBox

- Tải xuống VirtualBox miễn phí từ trang web chính thức:



Hình 21: VirtualBox

- <https://www.virtualbox.org/wiki/Downloads>
- Chạy file cài đặt và làm theo hướng dẫn trên màn hình.
- Khởi động lại máy tính sau khi cài đặt hoàn tất.

Bước 2: Tạo máy ảo

- Mở VirtualBox.
- Nhấp vào "New".
- Chọn loại hệ điều hành bạn muốn cài đặt (Windows 10 hoặc Windows Server 2012) và phiên bản.
- Nhấp vào "Next".
- Đặt tên cho máy ảo của bạn và chọn dung lượng RAM.
- Nhấp vào "Next".
- Chọn loại ổ cứng ảo bạn muốn sử dụng và dung lượng ổ cứng.
- Nhấp vào "Create".

Bước 3: Cài đặt Windows 10 hoặc Windows Server 2012

- Chọn máy ảo bạn vừa tạo và nhấp vào "Start".
- Chọn file ISO Windows 10 hoặc Windows Server 2012 bạn đã tải xuống.
- Làm theo hướng dẫn trên màn hình để hoàn tất quá trình cài đặt Windows.

Lưu ý:

- Bạn cần có file ISO Windows 10 hoặc Windows Server 2012 để cài đặt vào máy ảo. Bạn có thể tải xuống file ISO từ trang web chính thức của Microsoft:
 - Windows 10: <https://www.microsoft.com/en-us/software-download/windows10%20>
 - Windows Server 2012: <https://www.microsoft.com/en-us/evalcenter/download-windows-server-2012-r2>
- Bạn cần đảm bảo rằng máy tính của bạn có đủ cấu hình để chạy máy ảo. Bạn có thể tham khảo yêu cầu cấu hình tối thiểu cho Windows 10 và Windows Server 2012 trên trang web của Microsoft.

Dưới đây là một số hướng dẫn chi tiết hơn về cách cài đặt VirtualBox và cài Windows 10, Windows Server 2012:

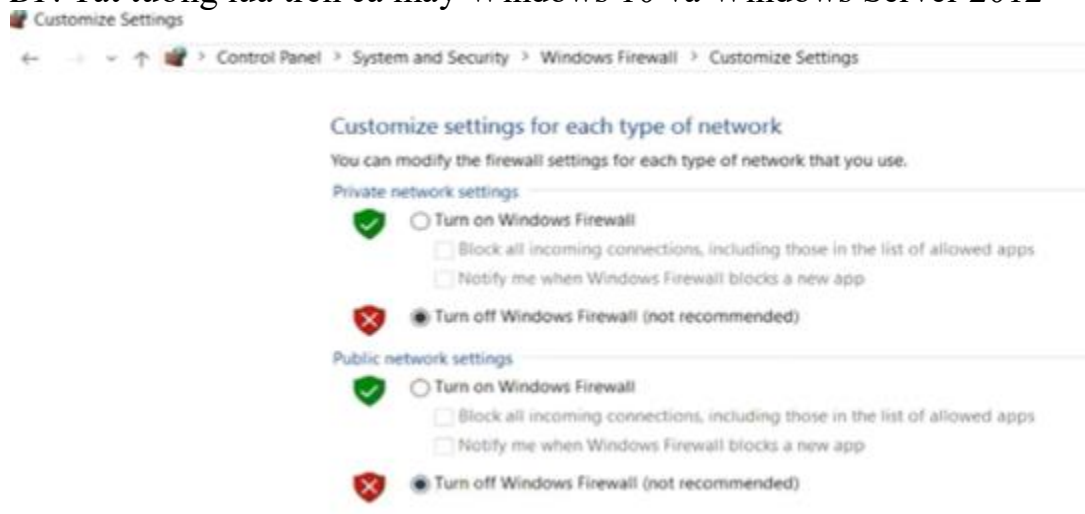
- **Cài đặt VirtualBox:** <https://tedu.com.vn/tag/Cai-dat-VirtualBox.html>
- **Cài đặt Windows 10 trên VirtualBox:** <https://www.thegioididong.com/game-app/cach-cai-windows-10-tren-may-ao-virtualbox-cuc-chi-tiet-1417548>
- **Cài đặt Windows Server 2012 trên VirtualBox:** <https://www.youtube.com/watch?v=aaZjwA-MrDI>

Ngoài ra, bạn cũng có thể tham khảo các video hướng dẫn trên YouTube:

- **Cài đặt VirtualBox:** [YouTube](#)
- **Cài đặt Windows 10 trên VirtualBox:** [YouTube](#)
- **Cài đặt Windows Server 2012 trên VirtualBox:** [YouTube](#)

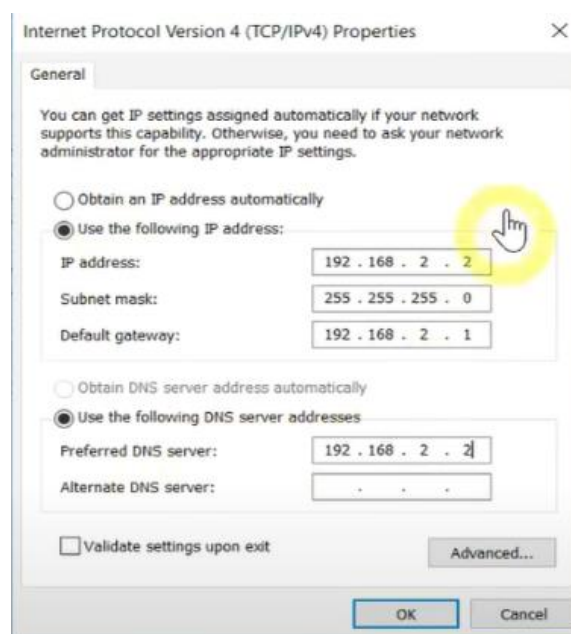
2. Tạo Domain Server

B1: Tắt tường lửa trên cả máy Windows 10 và Windows Server 2012



Hình 22: Tắt tường lửa

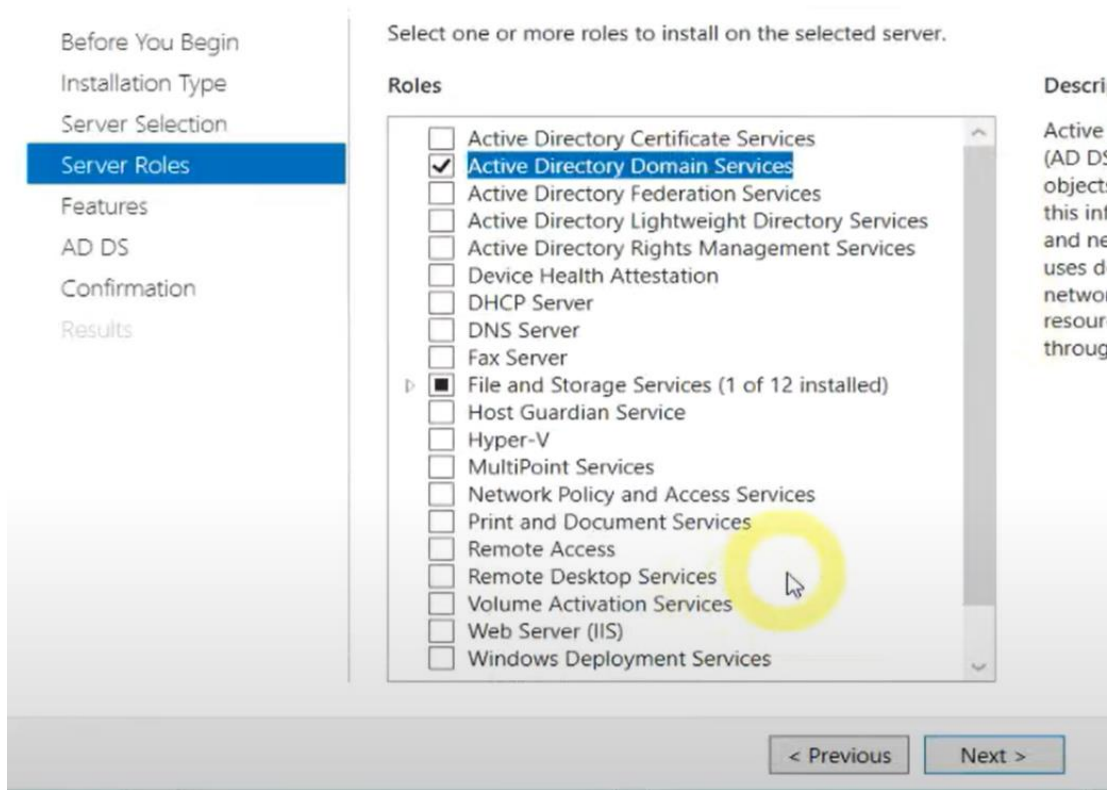
B2: Set IP cho máy Server



Hình 23: Set IP cho máy Server

B3: Add role để active Domain Server

Select server roles



Hình 24: Add role Active Directory Domain Services

B4: Nhấp vào "Install" để bắt đầu cài đặt vai trò Active Directory Domain Services.

B5: Sau khi cài đặt hoàn tất, nhấp vào "Close".

B6: Chọn "Server Manager" và nhấp vào "Manage" > "Add a new forest".

B7: Chọn "Root domain" và nhấp vào "Next".

B8: Nhập tên miền gốc (root domain name) vào ô "Root domain name". Ví dụ: attt.edu.vn

B9: Nhấp vào "Next".

B10: Nhập mật khẩu cho miền vào ô "Forest password" và "Confirm forest password".

B11: Chọn "Next".

B12: Nhấp vào "Next" để bắt đầu cài đặt miền.

B13: Sau khi cài đặt hoàn tất, nhấp vào "Finish".

B14: Khởi động lại máy tính.

B15: Sau khi khởi động lại, đăng nhập vào máy tính bằng tài khoản quản trị viên.

B16: Mở Server Manager.

B17: Chọn "Tools" > "Active Directory Users and Computers".

B18: Nhấp chuột phải vào tên miền và chọn "Properties".

B19: Chọn tab "NETBIOS name".

B20: Nhập tên NETBIOS cho miền vào ô "NETBIOS domain name".

B21: Nhấp vào "OK".

B22: Khởi động lại máy tính

3. Cách join domain từ Máy client với máy Server

Trước tiên, bạn phải set IP cho Windows 10 (Máy client).

Các bước thực hiện:

B1. Mở System Properties.

- Nhấp chuột phải vào biểu tượng "This PC" trên màn hình desktop và chọn "Properties".
- Hoặc, nhấn phím Windows + R để mở hộp thoại Run, nhập "sysdm.cpl" và nhấn Enter.

B2. Chọn tab "Computer Name".

B3. Nhấp vào "Change".

B4. Chọn "Join Domain" và nhấp vào "OK".

B5. Nhập tên miền vào ô "Domain name".

B6. Nhấp vào "OK".

B7. Nhập tên người dùng có quyền join domain vào ô "User name".

B8. Nhập mật khẩu cho người dùng đó vào ô "Password".

B9. Nhấp vào "OK".

B10. Khởi động lại máy tính.

Bạn có thể tham khảo cách cài domain và cách join tại link đây:

<https://youtu.be/1C0CUANXddg?si=YY2s5M6bDURLMO6u>

