HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

AN TOÀN HỆ ĐIỀU HÀNH[i]

BÀI THỰC HÀNH SỐ 01.01[ii]

KIỆN TOÀN AN TOÀN HỆ ĐIỀU HÀNH[iii]

Người xây dựng bài thực hành:

Đồng Thị Thùy Linh

HÀ NỘI, 2015

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Kiện toàn an toàn hệ điều hành
Module: An toàn hệ điều hành
Số lượng sinh viên cùng thực hiện: 01
Địa điểm thực hành: Phòng máy
Yêu cầu:

- Yêu cầu phần cứng:
  + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 2GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
  + VMware Worstation 9.0 trở lên
- Công cụ thực hành:
- Máy ảo VMware: windows 7 professional.
- Yêu cầu kết nối mạng LAN: không
- Yêu cầu kết nối mạng Internet: không
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

PHẦN 1. KIỆN TOÀN AN TOÀN HỆ ĐIỀU HÀNH

Máy tính đã trở thành một công cụ thiết yếu của mỗi cá nhân cũng như mỗi doanh nghiệp. Tuy nhiên, chúng cũng đứng trước nguy cơ bị đánh cắp thông tin, chiếm quyền kiểm soát, nhiễm mã độc.....Do vậy việc kiền toàn an toàn hệ điều hành đóng vai trò rất quan trọng nhằm bảo vệ máy tính khỏi các mối đe dọa nói trên.

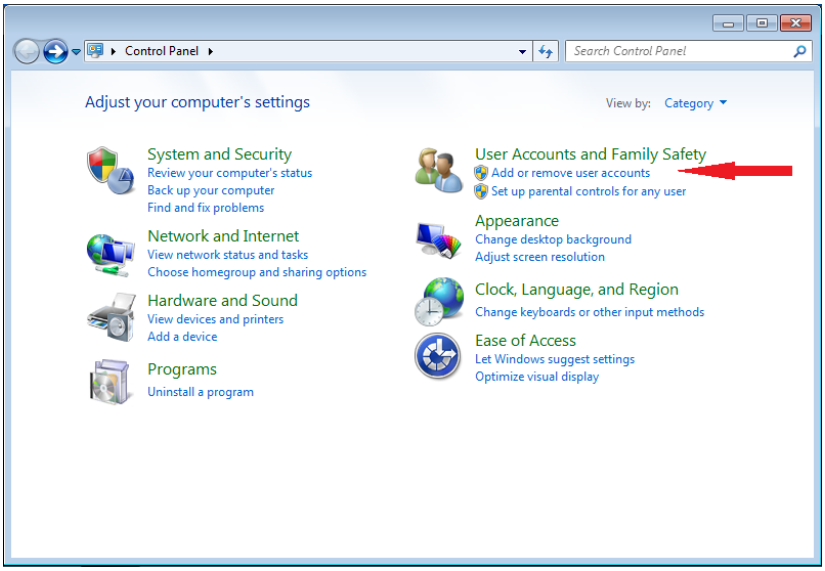
Bài thực hành này sẽ giới thiệu 5 nội dung chính trong kiện toàn an toàn hệ điều hành Windows 7 Professional: tạo tài khoản, thiết lập chính sách mật khẩu, cấu hình tường lửa, cập nhật, nhật ký.

1.1. Tạo tài khoản

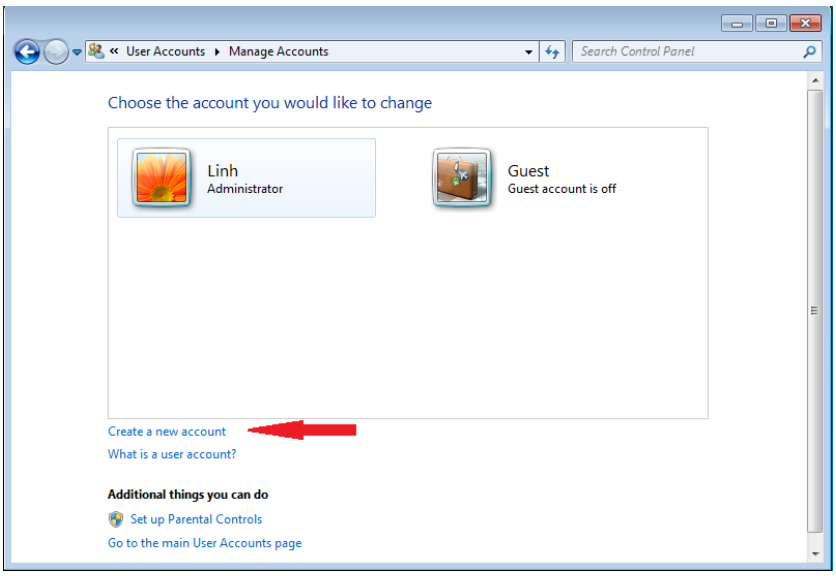
Như một số máy trạm khác, máy tính sử dụng hệ điều hành Windows 7 có thể được một hay nhiều người sử dụng, và Windows 7 đã được thiết kế để vận hành như một hệ điều hành đơn và đa người dùng. Windows 7 rất linh hoạt và có thể cung cấp hỗ trợ trong nhiều trường hợp khác nhau, trong đó mỗi người dùng sẽ được cấp một giấy phép phù hợp và một môi trường riêng. Sau đó mọi người dùng phải đăng nhập với mội tài khoản, mỗi tài khoản này có desktop, menu Start, thư mục Documents, History, Favorites và những tùy biến riêng. Tất cả những dữ liệu người dùng nằm trong thư mục Users của ổ đĩa hệ thống, trong đó mỗi tài khoản sẽ có một thư mục con được đặt tên theo tên của tài khoản này.

Bước 1: Nhấn vào nút Start có biểu tượng window ở góc dưới trái của màn hình

Bước 2: Nhấn vào Control Pannel

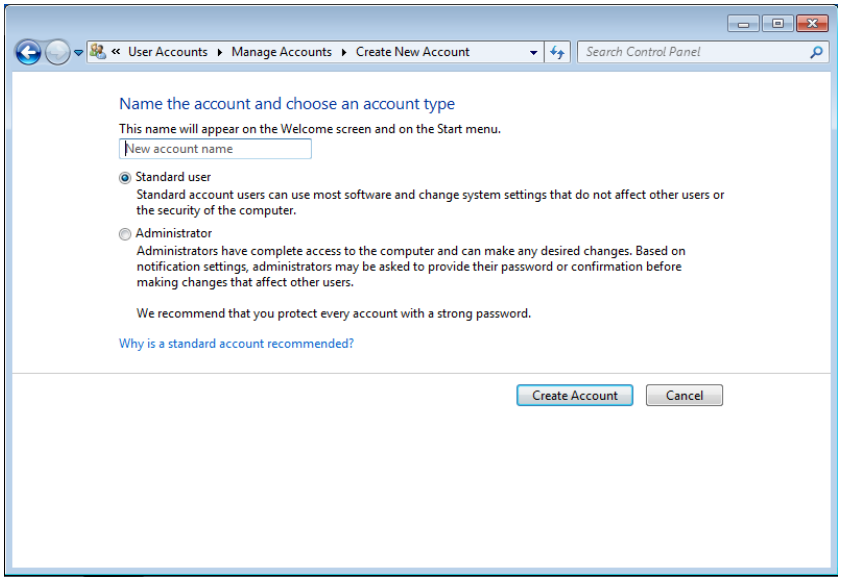


Bước 3: Nhấn vào mục Add or remove user accounts, sau đó cửa sổ Manage Accounts sẽ được mở ra như trong hình 2



Cửa sổ này sẽ hiện ra tất cả những tài khoản hiện có, để tạo một một tài khoản mới, người dùng Nhấn vào **Create a new account** ở phía dưới chỗ có mũi tên đỏ chỉ vào.

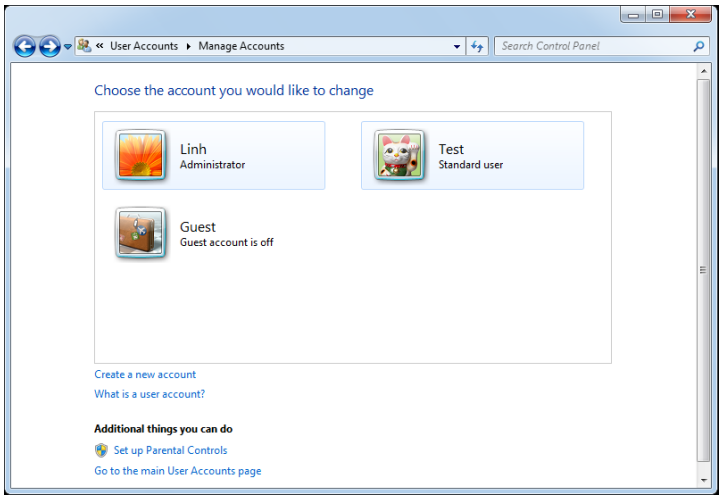
Bước 4: Cửa sổ Create New Account sẽ được mở ra như trong hình 3



Điền tên tài khoản mới mà Người dùng cần tạo trong phần New account name, sau đó Người dùng phải chọn loại . Có hai loại tài khoản: loại thứ nhất là Administrator, loại tài khoản này có quyền truy cập cao nhất vào máy tính và có thể làm tất cả những thay đổi như cài đặt phần mềm, tạo và xóa tài khoản. Còn loại thứ hai là Standard user, loại tài khoản này bị hạn hạn chế các quyền thiết lập và thay đổi trên máy tính. Để bảo vệ máy của Người dùng khỏi mã độc và những hành vi gây hại cho máy tính thì Người dùng chỉ nên để một tài khoản Administrator để đăng nhập khi cần thiết, còn tất cả tài khoản khác đều nên để Standard User. Các tài khoản này đều nên cài chế độ mật khẩu mạnh.

Sau khi đã đặt tên và chọn loại cho tài khoản Người dùng nên nhấn vào nút Create Account

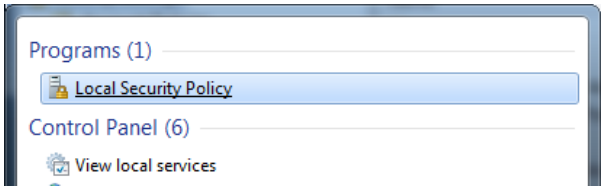
Bước 5:Sau đó tài khoản sẽ được tạo và sẽ được hiện thị trong cửa sổ Manage Accounts như trong hình

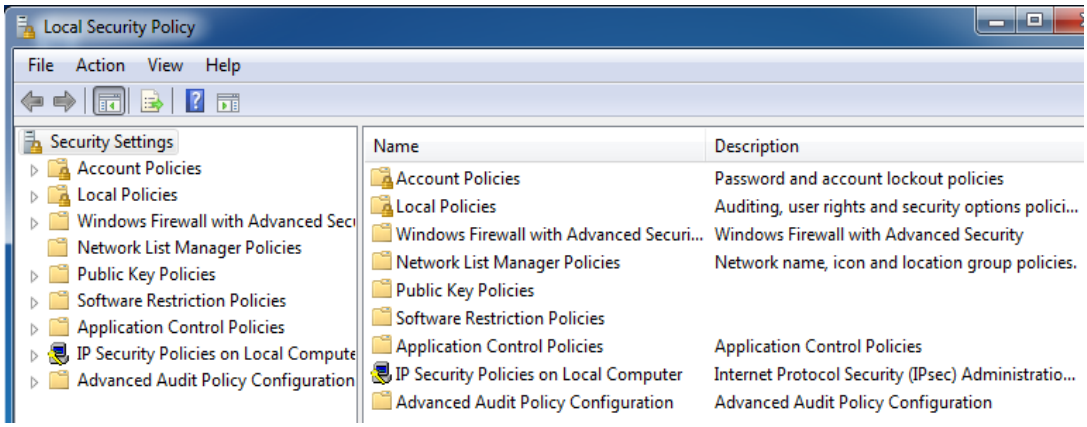


1.2. Thiết lập chính sách mật khẩu

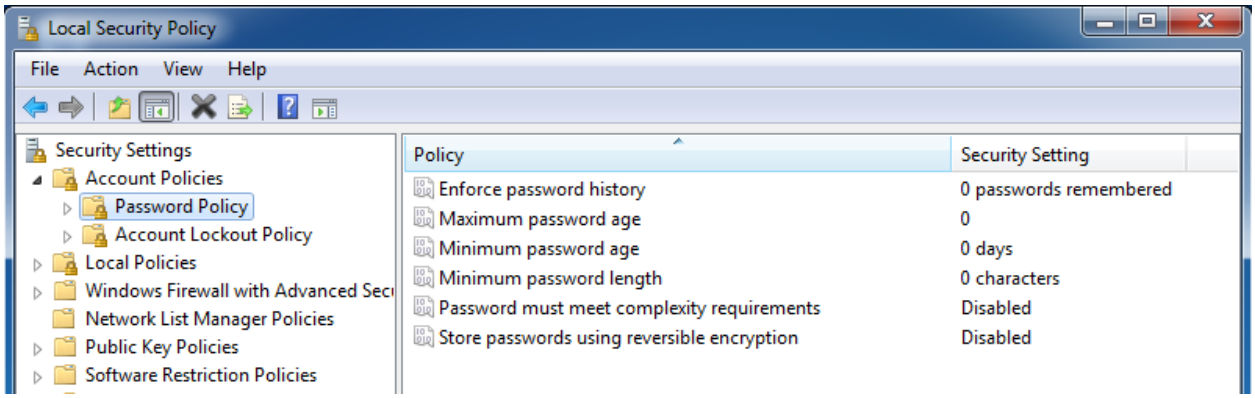
Người dùng có thể bảo vệ máy tính của mình bằng cách thay đổi các thiết lập chính sách mật khẩu như việc yêu cầu những người dùng thường xuyên thay đổi mật khẩu, đặt độ dài tối thiểu của mật khẩu, và yêu cầu họ sử dụng những mật khẩu khó. Người dùng phải đăng nhập tài khoản quản trị để thiết lập các chính sách mật khẩu.

Bước 1: Vào Start rồi vào search box "Local security policy"





Bước 2: Nhấn vào Account Policies > Password Policy rất nhiều tùy chọn sẽ hiện ra



Bảng dưới đây liệt kê các chính sách mật khẩu có sẵn, chức năng của mỗi chính sách, và cung cấp những khuyến nghị của Window đối với những thiết lập.

Chính sách	**Chức năng**	**Khuyến nghị của nhà cung cấp**
Enforce password history	Hạn chế việc người dùng tạo một mật khẩu mới nhưng lại giống với mật khẩu hiện tại của họ hoặc một mật khẩu đã được sử dụng gần đây. Để xác định có bao nhiêu mật khẩu được ghi nhớ, người dùng chỉ việc cung cấp một giá trị vào ô chọn. Ví dụ, với giá trị bằng 1 có nghĩa là chỉ có mật khẩu cuối cùng sẽ được ghi nhớ, với giá trị bằng 5 thì năm mật khẩu trước đó sẽ được ghi nhớ.	Nên chọn giá trị lớn hơn 1
Maximum password age	Thiết lập số ngày tối đa mà một mật khẩu được coi là hợp lệ. Vượt quá số ngày nà, người sử dụng sẽ phải thay đổi mật khẩu.	Tuổi thọ của mật khẩu tối đa nên để 70 ngày. Nếu thiết lập số ngày quá lớn sẽ tăng cơ hội cho kẻ tấn công có thể phá mật khẩu. Còn nếu thiết lập số ngày quá ít có thể gây phiền toái cho người sử dùng khi họ phải đổi mật khẩu quá thường xuyên.
Minimum password age	Thiết lập số ngày tối thiểu để có thể thay đổi một mật khẩu.	Đặt tuổi thọ mật khẩu tối thiểu để ít nhất 1 ngày. Như vậy, người dùng chỉ có

		thể thay đổi mật khẩu của họ một lần một ngày. Điều này sẽ hỗ trợ việc thực thi các thiết lập khác. Ví dụ, người quản trị đặt chế độ ghi nhớ năm các mật khẩu đã dùng thì điều này sẽ đảm bảo rằng người sử dụng chỉ có thể thay đổi mật khẩu sau năm ngày. Nếu tuổi thọ tối thiểu của mật khẩu được thiết lập là 0 thì người dùng không những có thể thay đổi mật khẩu của họ sáu lần một ngày và mà còn có thể sự dụng mật khẩu ban đầu của họ trong cùng một ngày.
Minimum password length	Thiết lập độ dài tối thiểu của một mật khẩu	Thiết lập độ dài từ 8 đến 12 ký tự (đáp ứng yêu cầu về độ khó của mật khẩu). Nếu người dùng không quan tâm đến việc một người nào đó trong văn phòng hoặc ở nhà sử dụng máy tính của mình thì người dùng có thể không sử dụng mật khẩu. Điều này thực chất sẽ bảo vệ máy tính của người dùng khỏi sự xâm nhập của kẻ tấn công từ mạng Internet hoặc các mạng khác tốt hơn là khi mgười dùng sử dụng một mật khẩu dễ đoán. Vì khi người dùng không sử dụng mật khẩu, Windows sẽ tự động ngăn chặn bất cứ đăng nhập vào máy tính của người dùng từ Internet hoặc các mạng khác.
Password must meet	Mật khẩu phải thỏa mãn các điều kiện sau:	Kích hoạt thiết lập này. Chức năng yêu cầu mật khẩu

complexity requirements	➢ Chứa ít nhất 6 ký tự ➢ Chứa tổ hợp của ít nhất 3 ký tự sau: chữ hoa, chữ thường, số, ký hiệu (vd: dấu chấm câu) ➢ Không chứa tên người dùng	khó giúp ngườ dùng tạo mật khẩu mạnh
Store passwords using reversible encryption	Lưu trữ mật khẩu mà không mã hóa	Luôn vô hiệu hóa chức năng này trừ khi người dùng sử dụng một chương trình yêu cầu phải bật chức năng này.

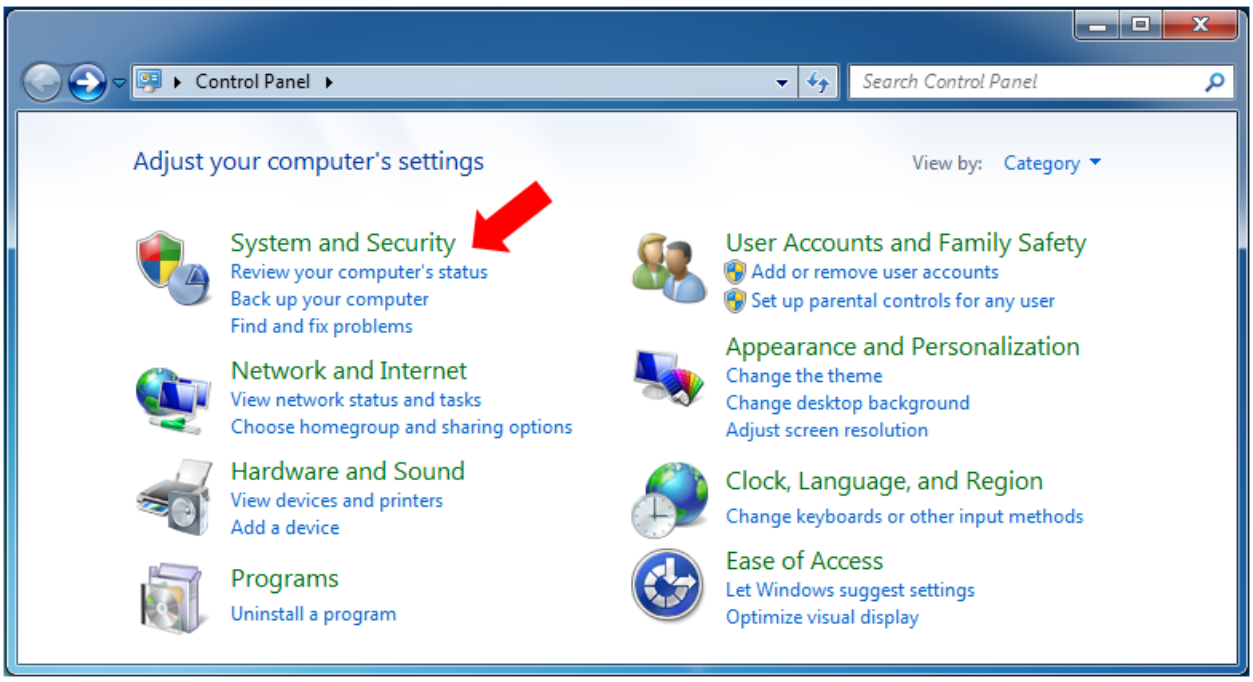
Sau khi hoàn thành các thiết lập người dùng vào Start>run rồi đánh "gpupdate /force" để cập nhật những thiết lập đó trên máy tính.

1.3. Cấu hình tường lửa

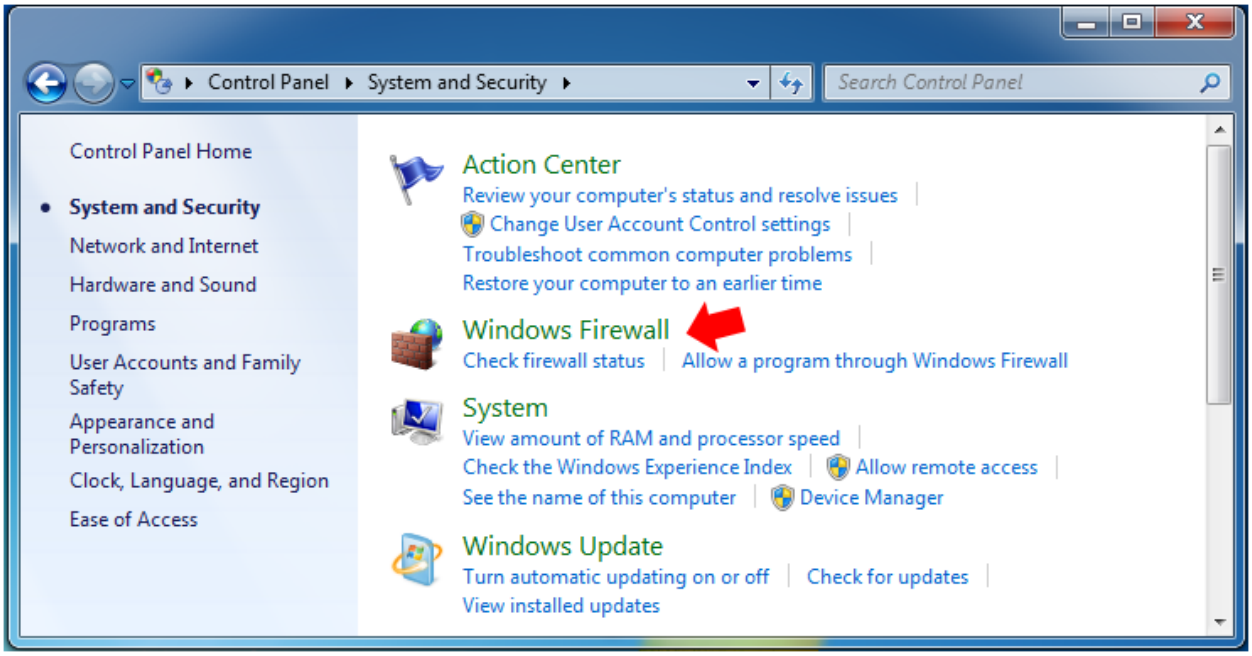
Tường lửa là một công nghệ dùng để lọc thông tin ra/vào máy tính hay hệ thống mạng của người dùng. Tất cả những thông tin vào máy tính của người dùng sẽ phải qua firewall, từ đây firewall sẽ kiểm tra thông tin rồi mới cho phép hoặc từ chối thông tin vào máy tính. Microsoft đã đưa những tính năng firewall vào những hệ điều hành của mình như **Windows XP,Vista**, **Windows 7 và Windows 8**

Sau đây là hướng dẫn cấu hình firewall trong Windows 7:

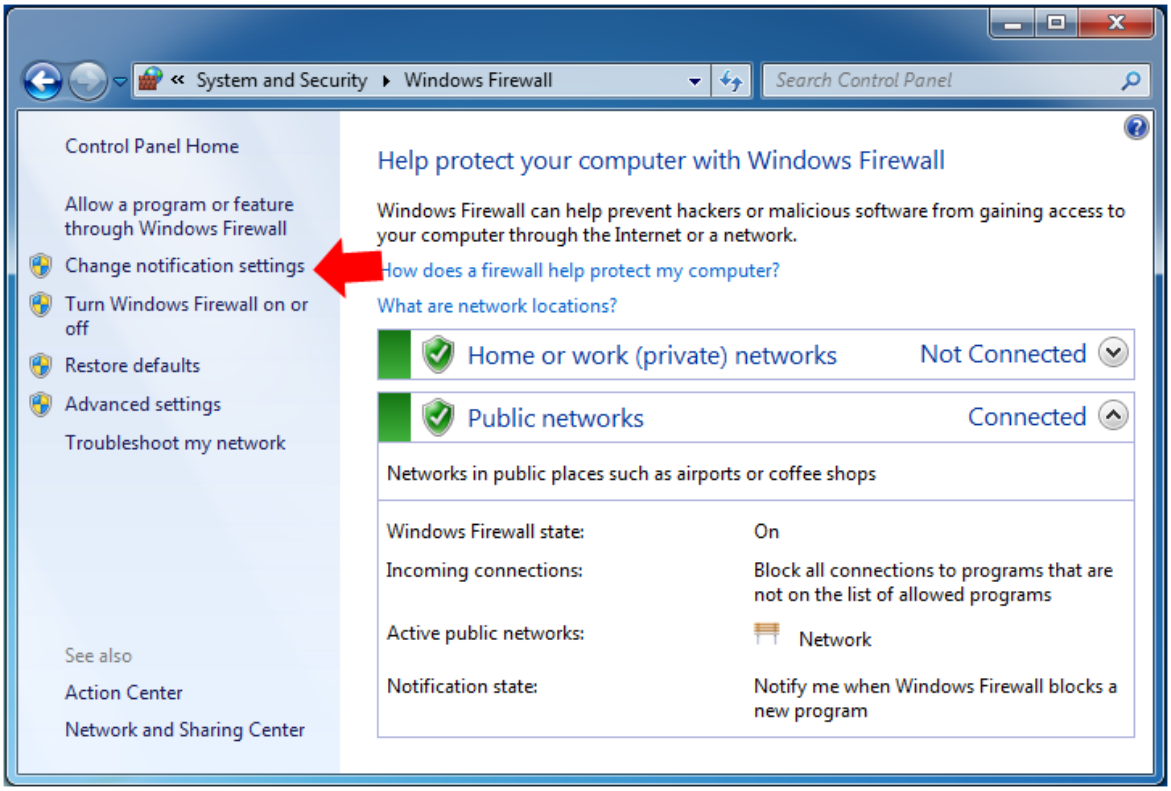
Bước 1: Người dùng phải đăng nhập máy tính với quyền administrative, truy cập theo đường dẫn **Start > Control Panel > System and Security.**



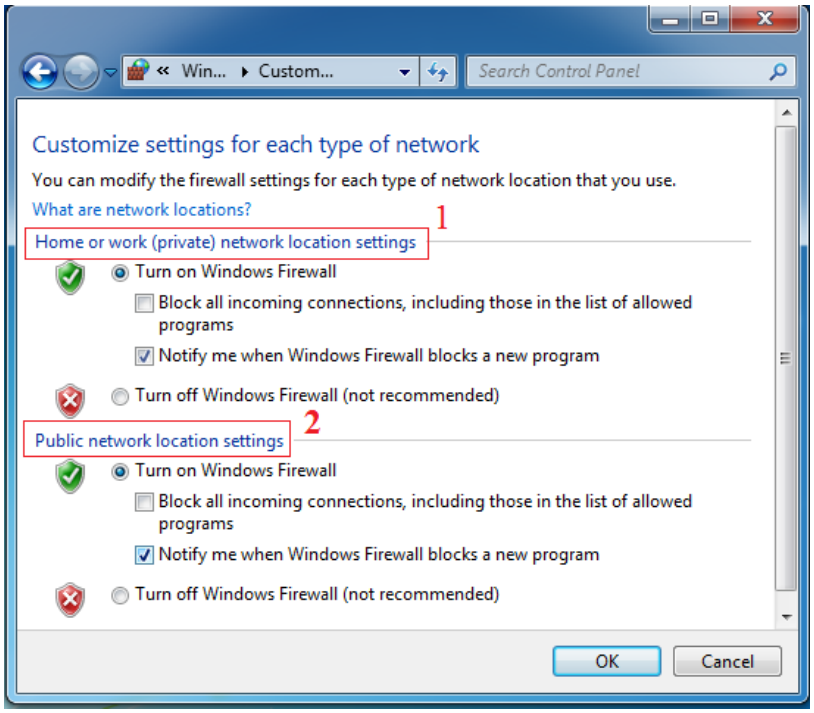
Bước 2: Trong cửa sổ **System and Security**, người dùng click vào **Windows Firewall**.



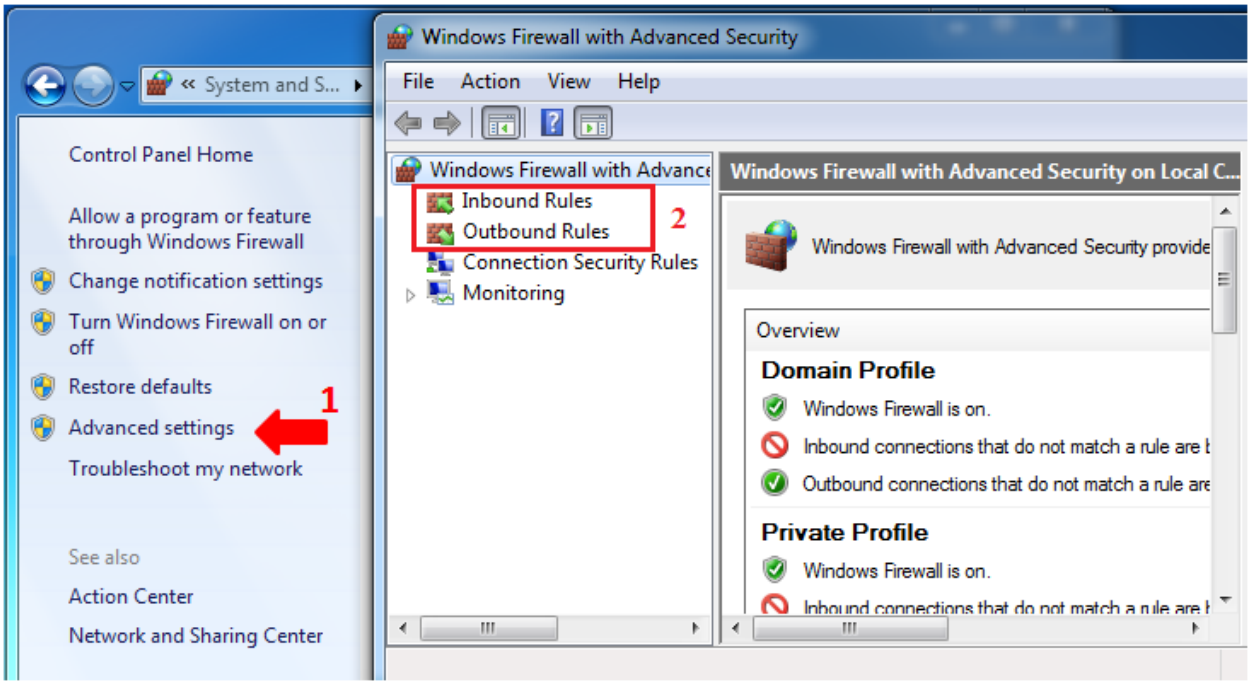
Bước 3: Ở cột bên trái giao diện, người dùng chọn Change notification settings để điều chỉnh cài đặt firewall.



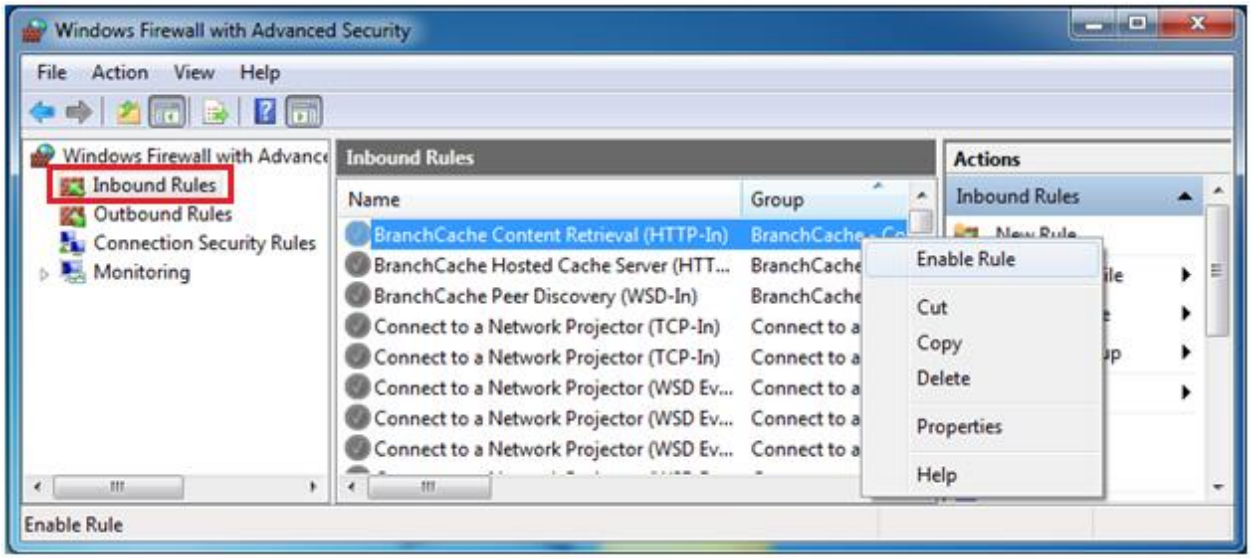
Bước 4: Tại đây, người dùng có thể tùy ý điều chỉnh bật hoặc tắt Firewall cho cả 2 chế độ Private và Public network



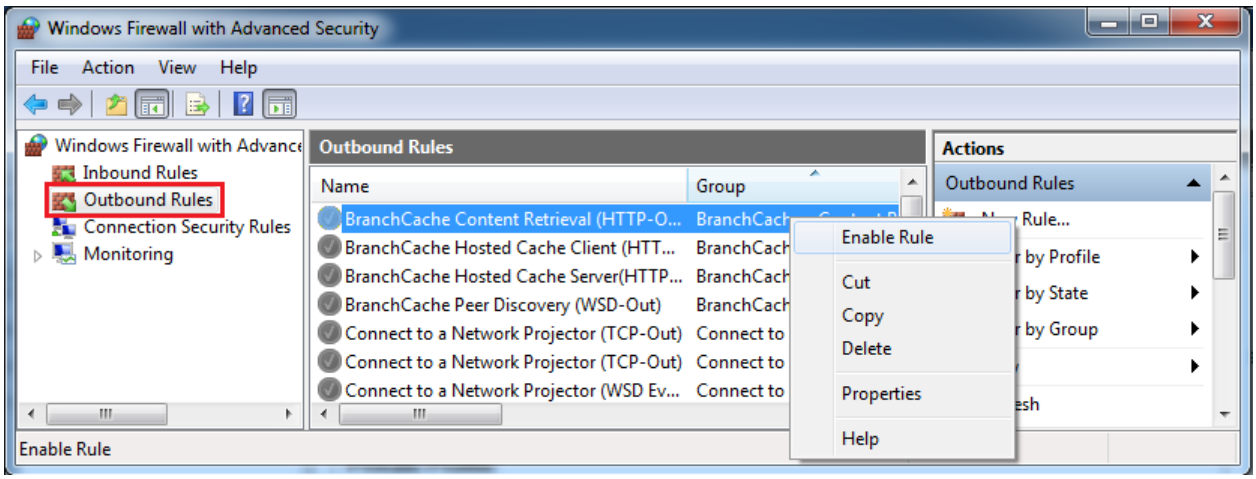
Bước 5: Người dùng có thể sử dụng Advance Setting để cấu hình firewall đối với luồng thông tin inbound và outbound tùy thuộc vào nhu cầu của mình.



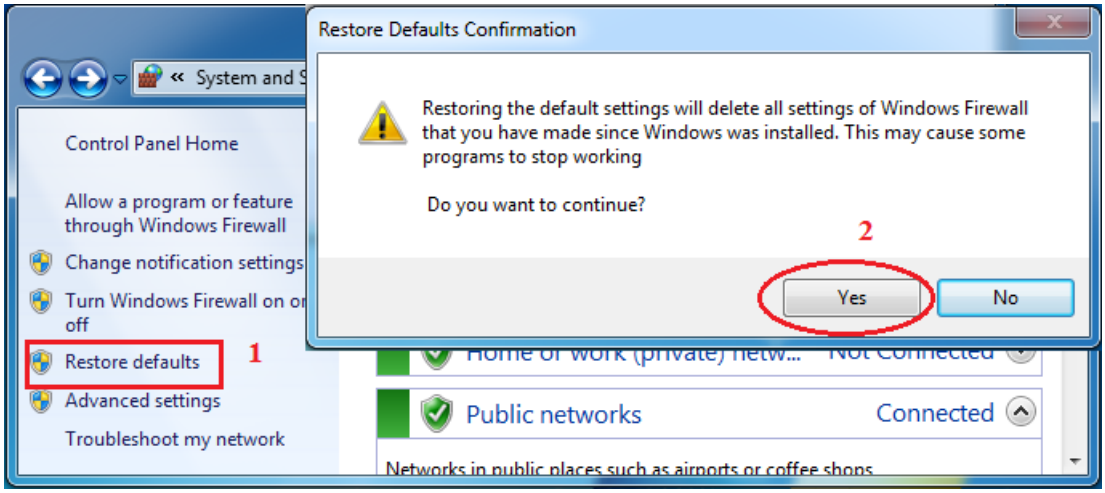
Khi nhấn vào Inbound Rules ở bên trái, người dùng sẽ thấy một danh sách Inbound Rules được hiển thị. Người dùng có thể kích hoạt hoặc vô hiệu hóa kết nối nào người dùng muốn bằng cách click chuột phải chọn Enable Rule/Disable Rule



Làm tương tự đối với Outbound Rules đối với các luồng thông tin đi ra.

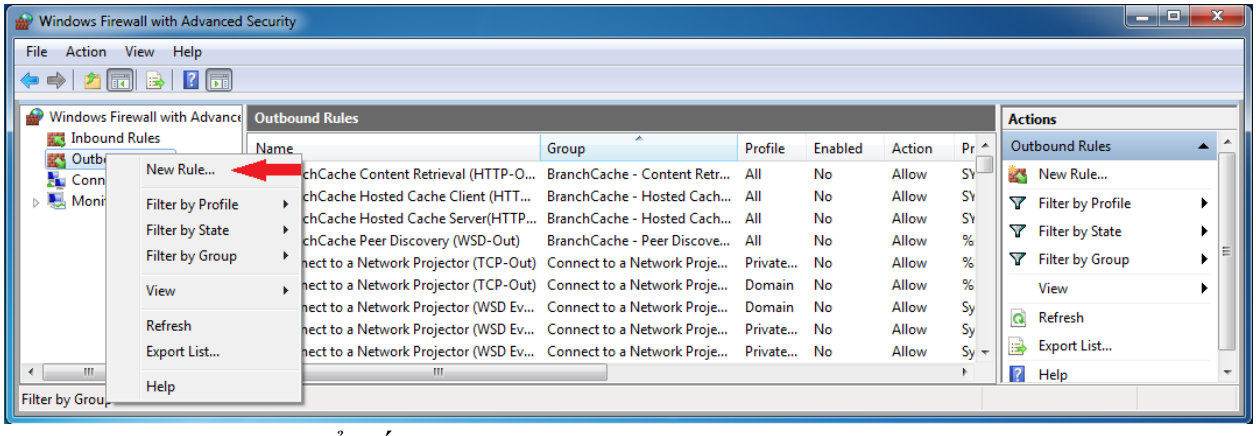


Hoặc trở về mặc định ban đầu thì hãy chọn Restore default và chọn Yes khi có thông báo xác nhận

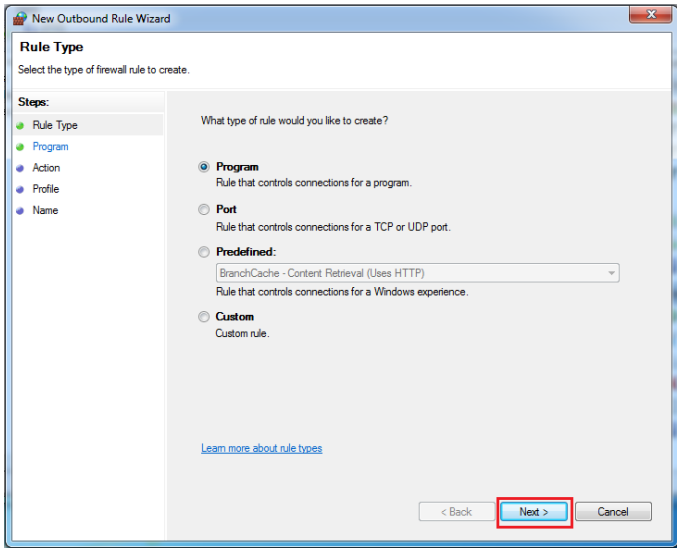


Ví dụ minh họa: ngắt kết nối Internet của ứng dụng trên windows 7

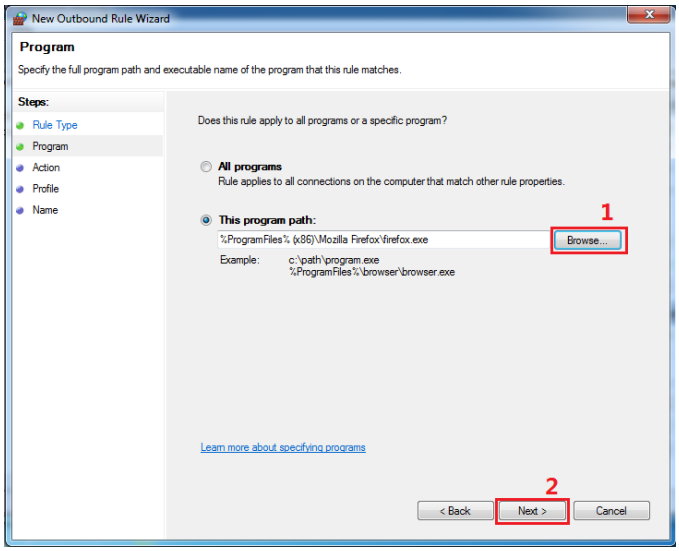
Bước 1: Tại đây bạn phải chuột vào Outbound Rules, sau đó chọn New Rule



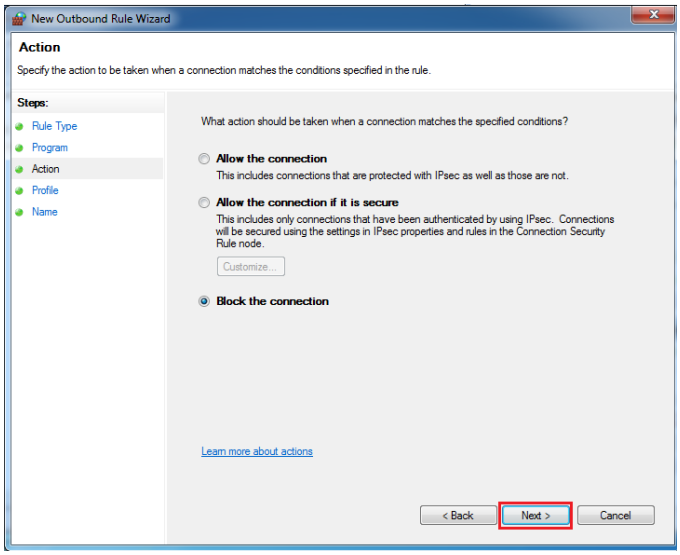
Bước 2: Chọn Next để tiếp tục



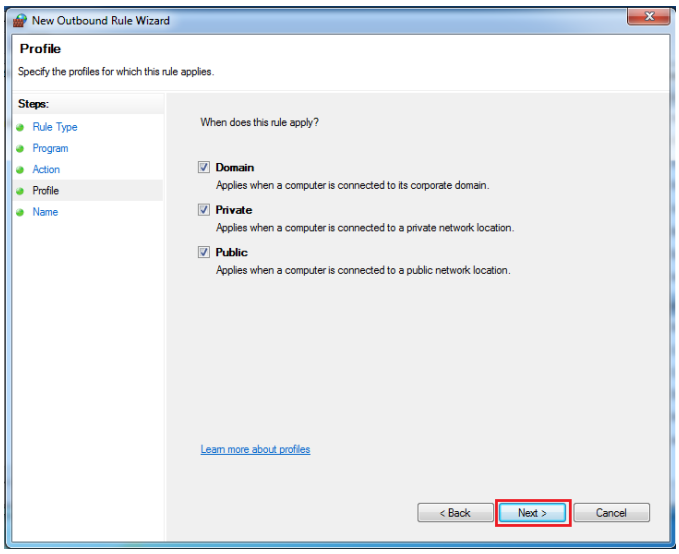
Bước 3: Tại phầnThis progarm parth chọn Browse để tìm đến ứng dụng cần chặn, ở đây ví dụ này, người dùng đã chọn trình duyệt Firefox để làm ví dụ. Chọn Next để tiếp tục



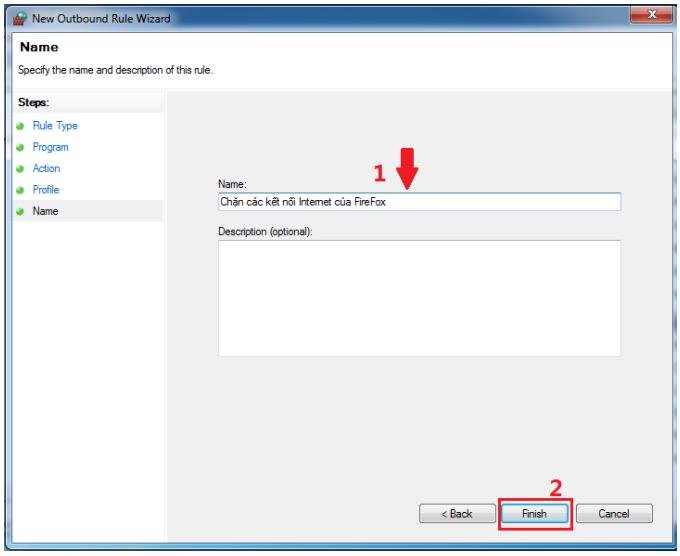
Bước 4: Chọn Block the connection để chặn tất cả các kết nối thông qua ứng dụng đã chọn, sau đó chọn Next để tiếp tục.



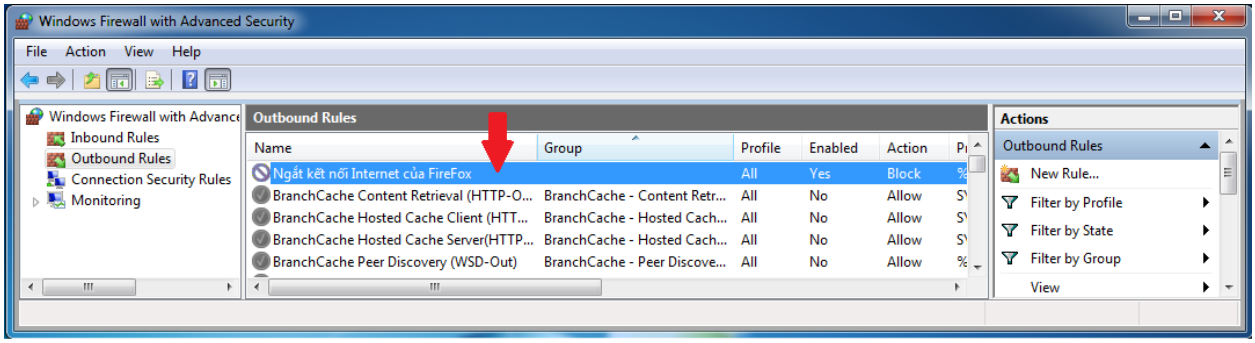
Bước 5: Chọn Next để tiếp tục



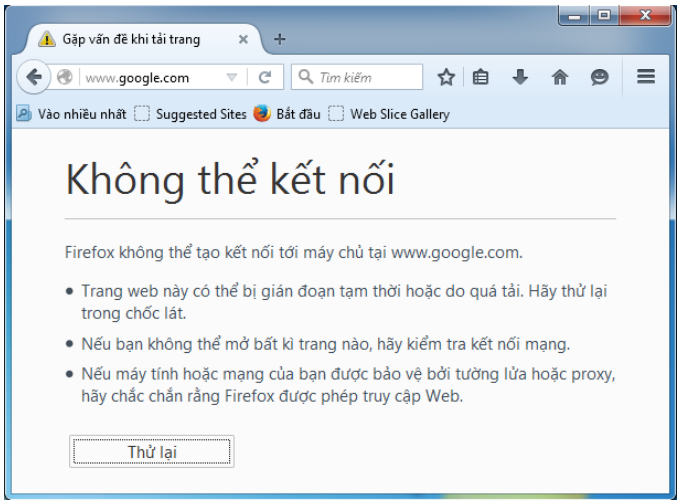
Bước 6: Tại đây nhập vào tên của luật đang tạo và những miêu tả ở dưới. Chọn Finsh để kết thúc



Sau khi tạo xong thì Rule sẽ xuất hiện trên cửa sổ của Outbond Rules như trong hình. Người dùng có thể tùy chỉnh luật này bằng cách nhấn chuột phải và chọn
properties.



Kiểm tra kết quả vừa làm được với trình duyệt Firefox

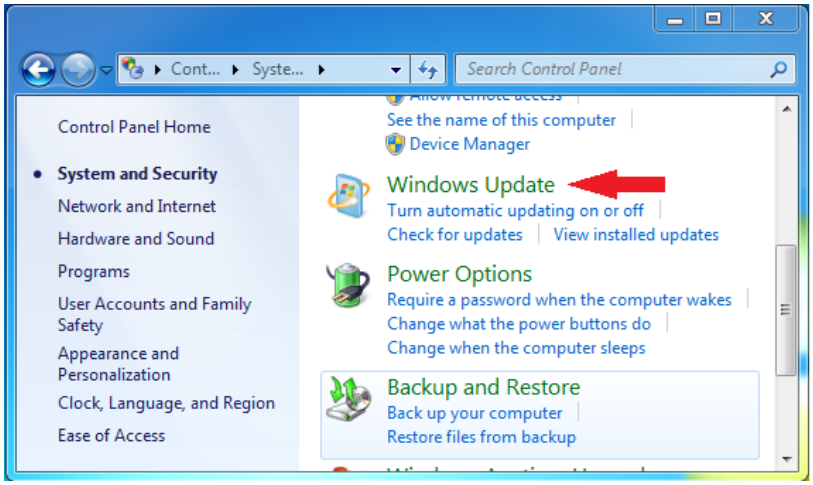


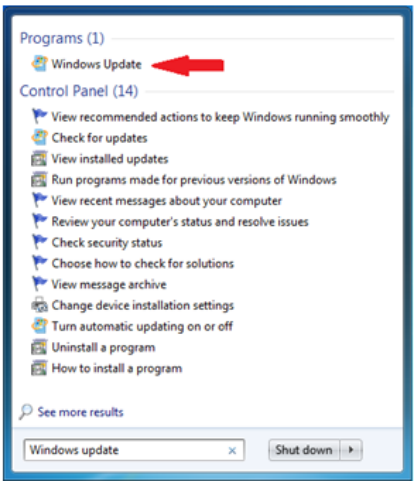
1.4. Cập nhật

Bước 1: Mở **Windows update.**

Đầu tiên người dùng chọn **Start** -> **Control Panel**->**System and Security**-> **Windows Update**

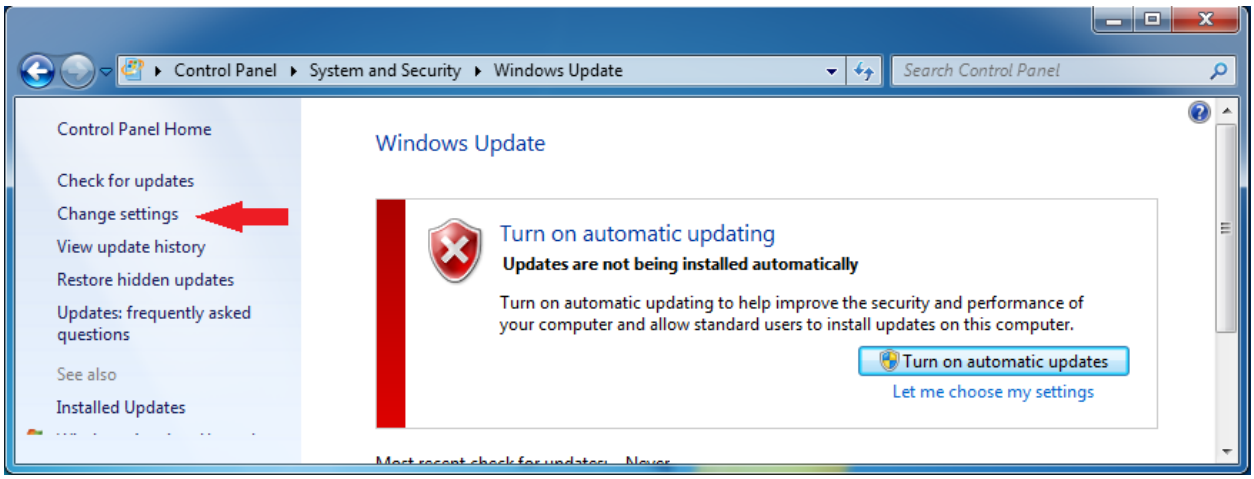
Hoặc người dùng có thể mở **Start** sau đó nhập từ khóa **Windows Update** vào ô **Search programs and files** và chọn **Windows Update.**



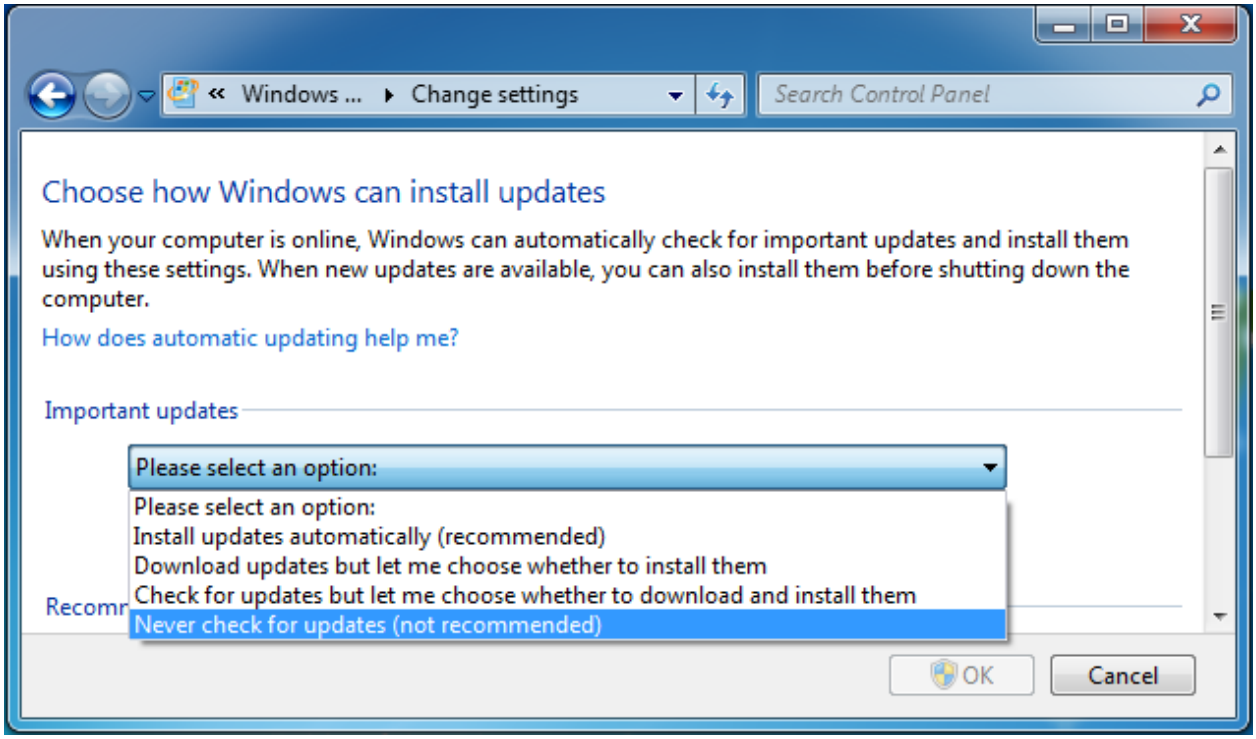


Bước 2: Thiết lập cho **Windows Update**

Trong menu bên trái người dùng chọn **Change settings.**



a) Trong phần Important updates (cập nhật quan trọng) người dùng có 4 lựa chọn, để bật hay tắt cập nhật hoặc cập nhật tự động:



- **Install updates automatically (recommended):** tự động tải updates về máy và tự cài. windows sẽ tự động kiểm tra, tải về và cài đặt bản cập nhật tại thời điểm người dùng chọn updates. Máy tính sẽ tự động cập nhật mà không không cần thực hiện bất kỳ thao tác nào, windows sẽ hiển thị thông báo yêu cầu Người dùng phải khởi động lại máy tính sau khi quá trình tải và cài đặt các bản cập nhật được thực hiện. Nếu Người dùng vắng mặt windows sẽ tự khởi động lại hệ thống.

- **Download updates but let me choose whether to install them:** tự tải updates nhưng không cài, windows sẽ kiểm tra các bản cập nhật mới và tải chúng về máy, hiển thị thông báo dưới khay hệ thống khi bản cập nhật mới được tìm thấy. Nhưng windows không tự động cài đặt. Nếu muốn cài đặt người dùng có thể nhấp

vào biểu tượng trên khay hệ thống, cài đặt bản cập nhật mới và khởi động lại máy tính.

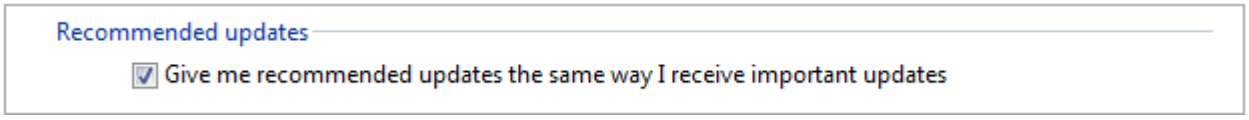
- **Check for updates but let me choose whether to download and install them:** chỉ thông báo có update nhưng không tải. Windows sẽ kiểm tra các bản cập nhật và hiển thị thông báo dưới khay hệ thống, nó không tải bản cập nhật về máy cho đến khi người dùng yêu cầu.

- **Never check for updates (not recommended):** tắt tính năng updates. Windows sẽ không tự động kiểm tra các bản cập nhật, tắt hoàn toàn tính năng updates.

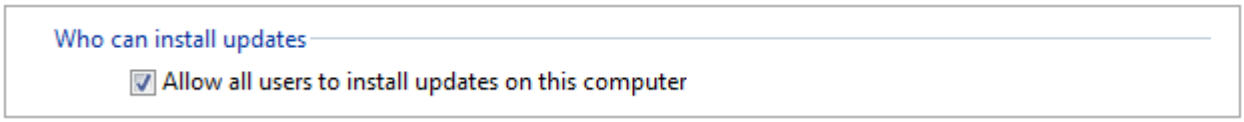
* Để bật tính năng updates người dùng chọn cách bật theo nhu cầu trong 3 lựa chọn đầu. Nếu chọn **Install updates automatically (recommended)** thì người dùng tùy chỉnh thêm thời gian tự động updates.

* Để tắt tính năng updates người dùng chọn **Never check for updates (not recommended).**

b) Trong phần Recommended updates (cập nhật đề nghị) người dùng có thể đánh dấu vào ô vuông trước **Give me recommended updates the same way I receive important updates** nếu muốn cập nhật đề nghị để được cài đặt cùng với cập nhật quan trọng.



c) Trong phần **Who can install updates** (ai có thể cài đặt bản cập nhật). Nếu không chọn phần này người dùng có thể cài đặt bản cập nhật chỉ khi Người dùng đang đăng nhập với tài khoản quản trị. Nếu người dùng đánh dấu chọn vào ô vuông trước **Allow all users to install updates on this computer** sẽ cho phép tất cả các tài khoản trên máy tính đều có thể cài đặt các gói update vừa tải.



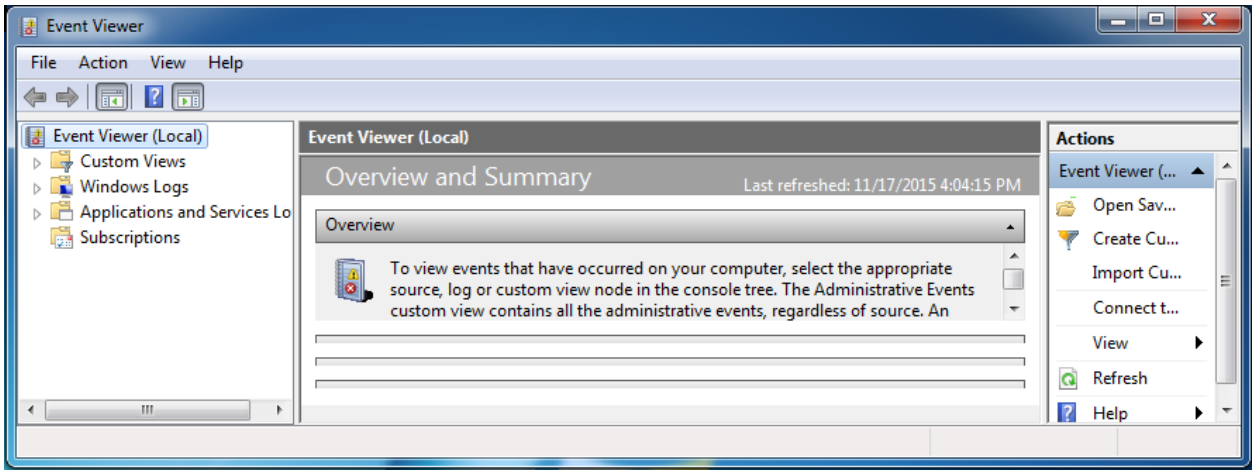
Bước 3: Sau khi thiết lập xong người dùng nhấn **OK** để lưu lại thay đổi.

1.5. Nhật ký

Event viewer là một công cụ tích hợp trong Windows cho phép Người dùng xem lại các sự kiện đã xảy ra trong hệ thống một cách chi tiết với nhiều tham số cụ thể như: user, time, computer, services… Các sự kiện rời rạc được lọc lại thành

những sự kiện giống nhau giúp chúng ta lấy được những thông tin cần thiết một cách nhanh nhất.

Để vào **Event viewer** Người dùng nhấn vào **Start -> Control Panel-> System and Security->Administrative Tools->Event Viewer**



Event Viewer của Windows 7 gồm có ba panel:

- Panel bên trái để chọn các thông tin nhằm từ Custom Views,Windows Logs, Applications v Services Logs và Subscriptions.
- Panel giữa hiển thị các thông tin về nút được chọn.
- Panel phải (Actions) cho phép Người dùng tạo các bản ghi, tạp các khung nhìn, định vị các sự kiện được chọn và tìm kiếm sự trợ giúp.

Khi khởi chạy Event Viewer, panel trung tâm của nó sẽ hiển thị tổng quan về hệ thống của Người dùng. Phần tóm tắt về các sự kiện quản trị (Summary of Administrative Events) sẽ hiển thị các thống kê về các lỗi, cảnh báo, các thông tin và các sự kiện thẩm định thành công theo tuần, ngày, giờ.

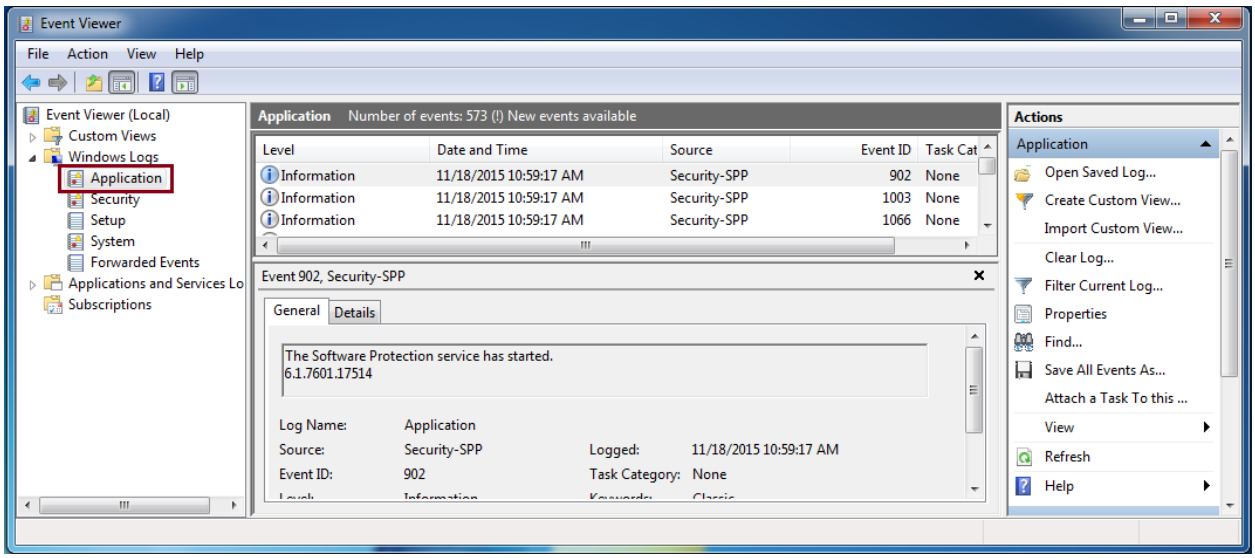
Kích dấu cộng (+) bên cạnh một mục nào đó để xem các sự kiện của mục đó. Kích đúp vào một sự kiện, sự kiện này sẽ được mở ở panel giữa.

Khi mở một sự kiện, panel bên phải sẽ cung cấp các tùy chọn bổ sung cho sự kiện, gồm có khả năng đính kèm một nhiệm vụ cho sự kiện, chẳng hạn như việc gửi một email khi một sự kiện khác của cùng kiểu xảy ra – một lỗi nghiêm trọng.

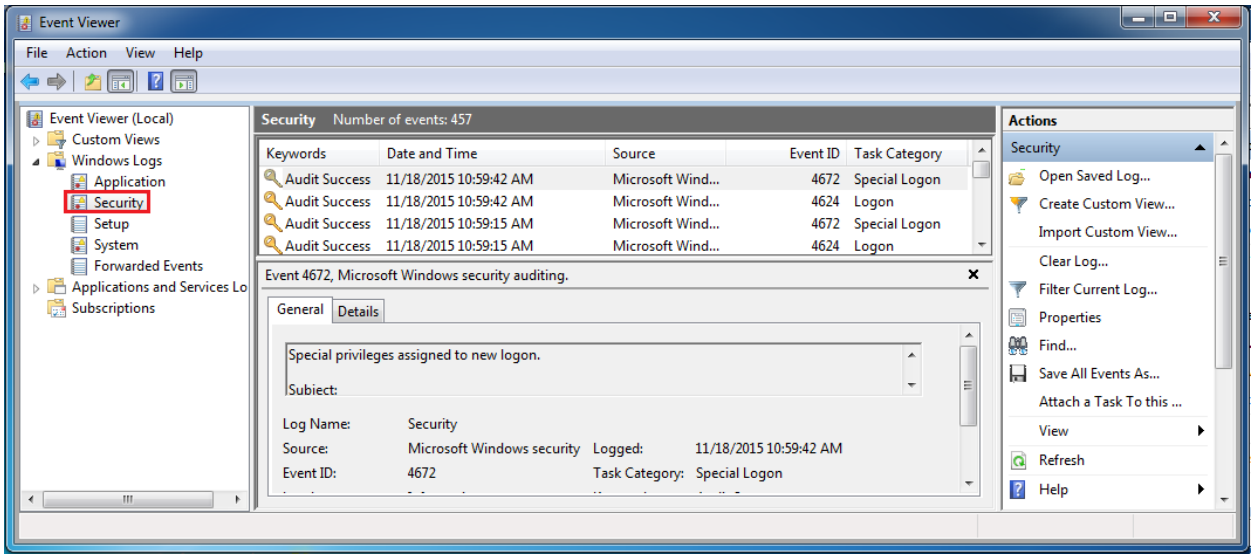
Xem lại các bản ghi của Windows

Mở thư mục **Windows Logs** Người dùng có thể xem các mục bản ghi cho các ứng dụng, các sự kiện bảo mật, thiết lập, hệ thống hay các sự kiện đã được chuyển tiếp.

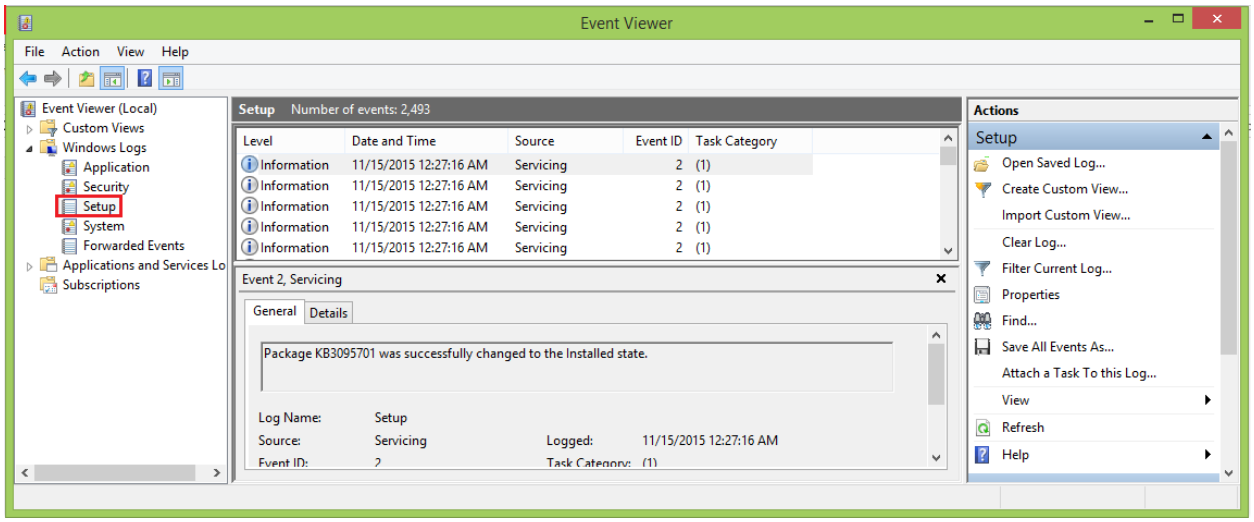
Sử dụng bản ghi **Applications** có thể tìm ra thời điểm khi một dịch vụ khởi chạy hay dừng, hoặc có thể khắc phục sự cố các vấn đề với dịch vụ chẳng hạn như Backup.



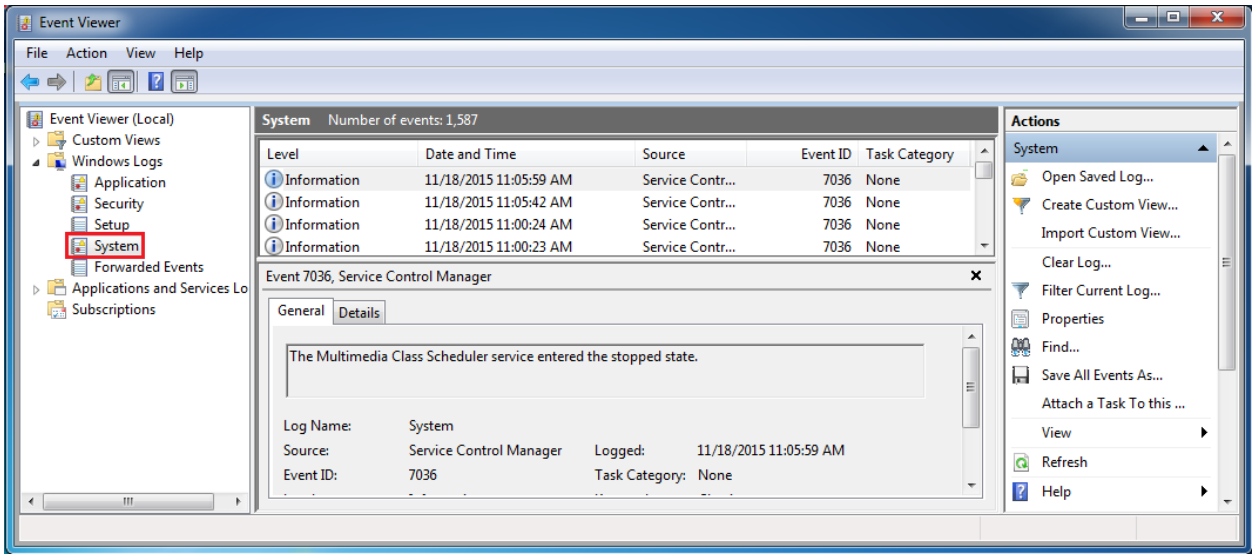
Sử dụng bản ghi **Security** có thể xác định xem chế độ bảo mật đăng nhập và đăng xuất hiện có làm việc hay không.



Sử dụng bản ghi Setup có thể xác định được thời điểm các nâng cấp của Windows được cài đặt.



Sử dụng bản ghi System có thể biết được các hành động duy trì, các vấn đề với bản ghi giao dịch.



Bản ghi Forwarded Events liệt kê các sự kiện mà Người dùng đang chia sẻ với các hệ thống khác.

Các bản ghi Applications và Services :Windows 7, cũng giống như Windows Vista, đưa các bản ghi Applications và Services vào thư mục của người dùng trong Event Viewer. Media Center, Windows PowerShell, và Microsoft Windows tất cả đều có các bản ghi riêng cũng như các sự kiện phần cứng, Internet Explorer, Key Management Services, Windows Backup, và các tiện ích Windows khác. Bằng cách mở bản ghi Backup/Operational, Người dùng có thể thấy trạng thái của các công việc backup gần đây. Mở bản ghi cho một tính năng nào đó của Windows 7 (Microsoft>Windows>featurename) Người dùng có thể thấy thời điểm khi một tính năng nào đó được sử dụng hoặc các vấn đề được báo cáo gần đây nhất

[i] Lấy tên theo tên của module thực hành trong danh sách đã phân công

[ii] Đánh số theo số thứ tự bài thực hành trong từng module. Số thứ tự của module gồm 2 chữ số và số thứ tự của bài trong module gồm 2 chữ số.

[iii] Lấy đúng tên của bài thực hành trong danh sách đã phân công