Fpt University

FPT POLYTECHNIC

Chương 6
Bảo mật

Mục tiêu bài học

- Biết tạo tài khoản với những quyền khác nhau
- Quản lý được tài khoản người dùng
- Thiết lập được tường lửa để ngăn chặn những kết nối ngoài ý muốn
- Thiết lập chế độ tự động update của Windows
- Biết các chế độ bảo mật của mạng không dây và cấu hình được trên access point.

Quyền người dùng

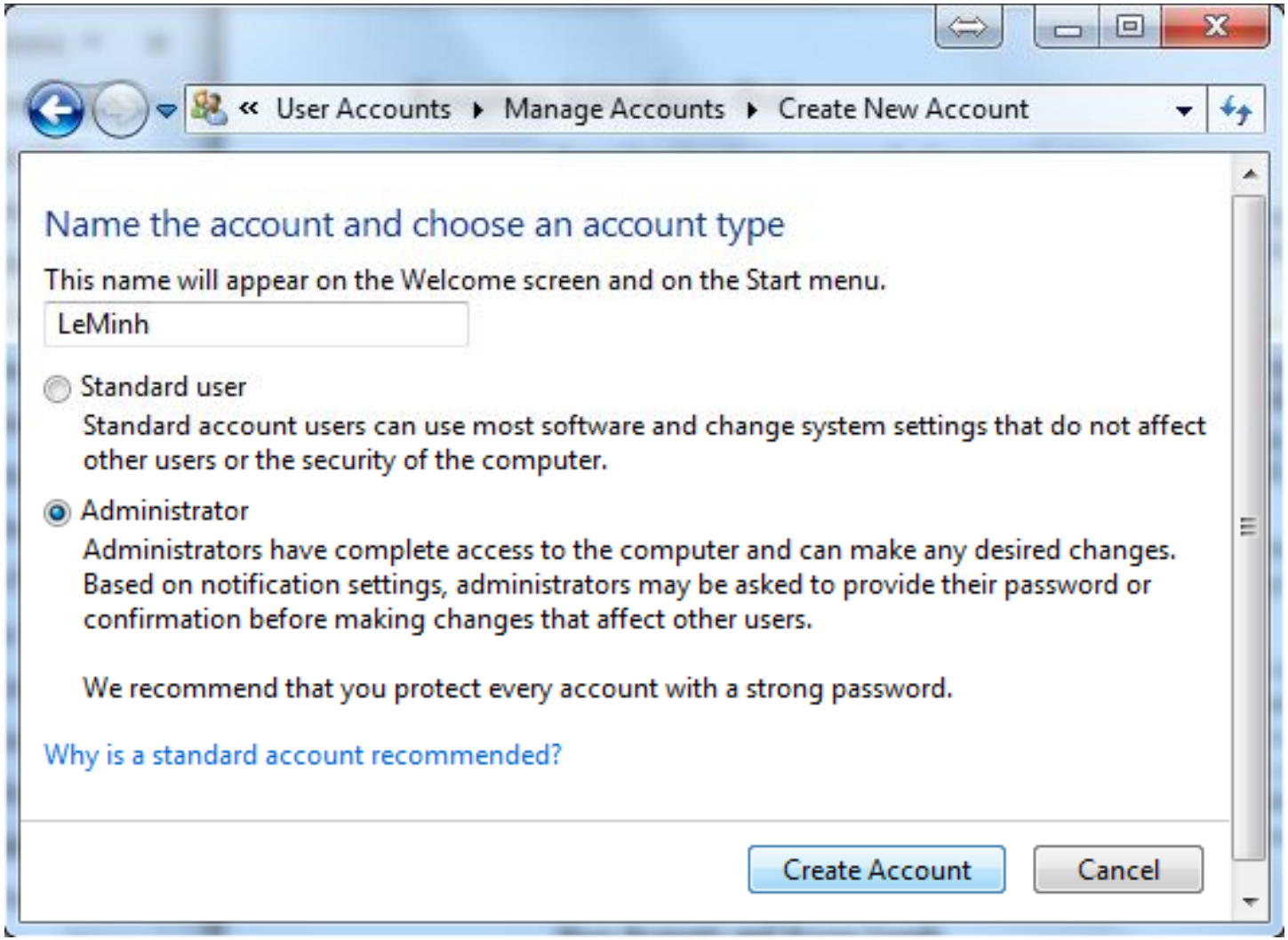
- Một máy tính có thể có nhiều người dùng, để tránh việc người dùng này làm thất lạc hoặc thay đổi dữ liệu của người kia, ta có thể phân quyền thông qua tạo tài khoản người dùng.
- Bạn phải đăng nhập với quyền administrator mới có quyền thực hiện chức năng này
- Trên Windows XP, Vista, Windows7 có hai loại tài khoản

Tài khoản	Ý nghĩa
Administrator	Quản trị viên – Toàn quyền
Standard user/Limited	User - Giới hạn quyền

Tạo Account phân quyền truy cập

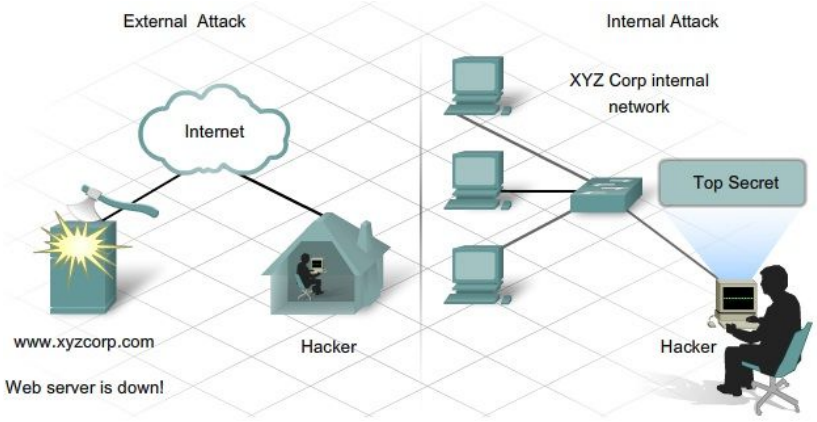
- Với tài khoản dạng Administrator, bạn có toàn quyền sử dụng tất cả các tài nguyên có trên máy, bao gồm cả tài nguyên của account dạng administrator khác.
- Với tài khoản User (Limited/ Standard) bạn chỉ có toàn quyền trên những tài nguyên do bạn tạo ra, còn lại những tài nguyên khác có trên máy, bạn chỉ có quyền đọc (read).
- Để tạo account mới, vào Control Panel chọn chọn Add or remove user accounts trong mục User Accounts and Family Safety. Chọn Create a new account. Đặt tên cho account cần tạo, chọn kiểu tài khoản (toàn quyền/giới hạn quyền) bằng lựa chọn Administrator hoặc Standard user/Limited, cuối cùng bấm chọn Create Account để tạo
- Sau khi tạo xong tài khoản, bạn cũng có thể thiết lập mật khẩu cho tài khoản vừa tạo bằng cách chọn tên tài khoản và chọn mục Create a password

Tạo Account phân quyền truy cập



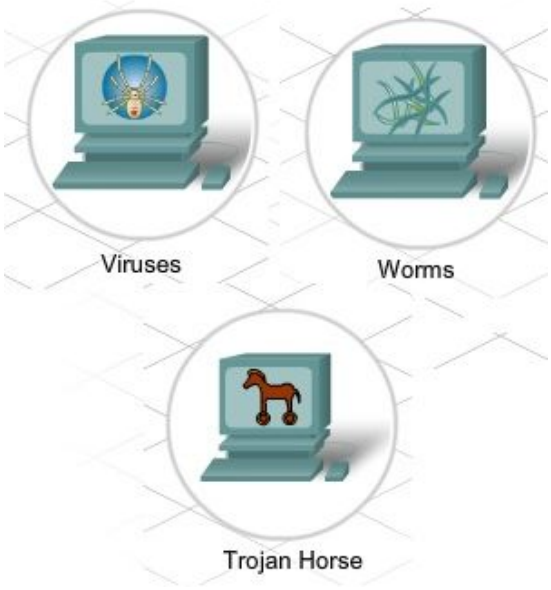
Nguồn của xâm nhập mạng

- Các mối đe dọa an toàn xuất phát từ bên trong và bên ngoài.
- Đe dọa từ bên ngoài: Các mối đe dọa bên ngoài xuất phát từ các cá nhân làm việc bên ngoài tổ chức. Họ không có quyền truy cập tới hệ thống máy tính hoặc mạng. Tấn công qua Internet, Wireless hoặc Dialup Access Server.
- Các đe dọa từ bên trong: xảy ra khi một người có quyền truy cập tới mạng qua tài khoản hoặc truy cập vật lý tới các thiết bị mạng. biết chính sách, người, biết thông tin nào là có giá trị , cách lấy nó.



Virus, Worm và Trojan Horses

- Chúng có thể phá hỏng hệ thống, phá hủy dữ liệu, cấm truy cập mạng, hệ thống hoặc các dịch vụ. Chúng cũng có thể chuyển tiếp dữ liệu và thông tin cá nhân chi tiết từ các nạn nhân đến các kẻ tội phạm. Chúng có thể phát tán tới các máy khác kết nối qua mạng.



Virus

- Virus là 1 chương trình mà chạy và phân tán bằng cách sửa các chương trình hoặc các file khác.
- Virus cần được kích hoạt. Khi kích hoạt chúng nhân bản và phân tán.
- Virus đơn giản có thể nhanh chóng sử dụng bộ nhớ và làm cho hệ thống dừng hoạt động.
- Loại virus nguy hiểm có thể được lập trình để xóa hoặc làm hỏng các file trước khi chúng phát tán.
- Virus có thể được truyền qua các file attach, các file được download, IM hoặc qua CD, USB.

Worm

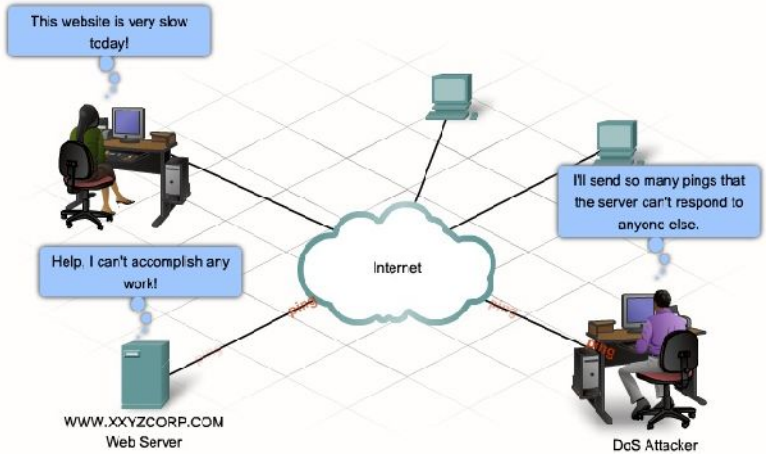
- Worm tương tự như virus, nhưng chúng không như virus không cần tự nó chứa một chương trình.
- Worm sử dụng mạng để gửi và copy nó đến bất kỳ máy nào được kết nối.
- Worm có thể chạy độc lập và phân tán nhanh. Chúng không cần yêu cầu kích hoạt hoặc tác động của con người.
- Tự động phân tán các Worm có tác động lớn hơn virus đơn và có thể ảnh hưởng phần lớn của Internet nhanh chóng.

Trojan Horses

- A Trojan Horses là một chương trình không tự động tái tạo và được viết giống như một chương trình hợp pháp, trong thực tế nó sử dụng một tool để tấn công.
- Trojan dựa vào giao diện của nó để đánh lừa nạn nhân để khởi tạo chương trình.
- Nó có thể vô hại hoặc chứa các mã nguồn có thể phá hủy nội dung của đĩa cứng máy tính.
- Trojan có thể tạo backdoor vào hệ thống để cho phép hackers dành quyền truy cập.

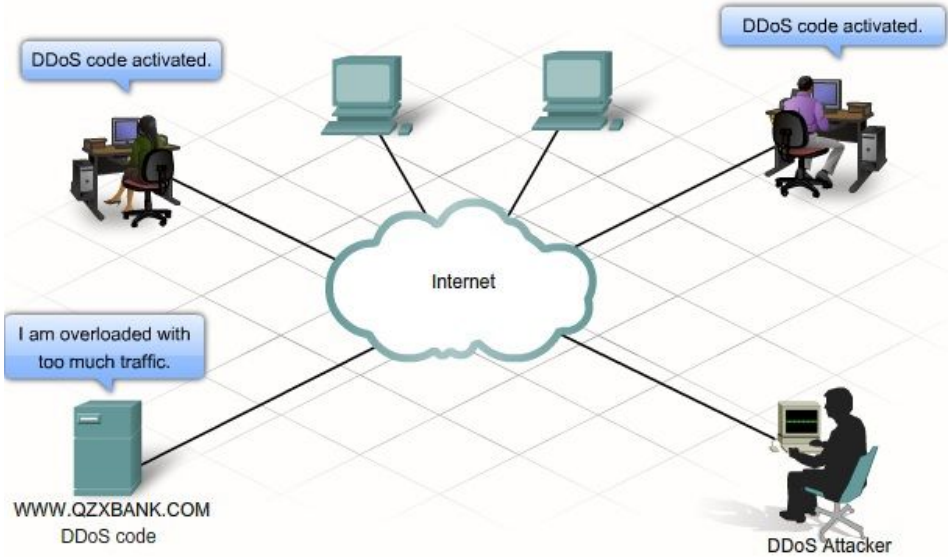
Tấn công từ chối dịch vụ DoS (Denial of Service)

- DoS là tấn công công kích vào một máy tính hoặc 1 nhóm máy tính cụ thể với mục đích là cấm các dịch vụ đến các người dùng đang chờ. DoS tấn công có thể đích là hệ thống người dùng đầu cuối, các server, router và các liên kết mạng.
- Thông thường, DoS tấn công tìm để:
  - Làm tràn ngập một hệ thống hoặc một mạng với các gói tin để ngăn cản các lưu lượng mạng của luồng.
  - Phá vỡ kết nối giữa client và server để ngăn chặn truy cập các dịch vụ.
- Có 2 loại tấn công DoS là:
  - SYN (synchronous) Flooding
  - Ping of death



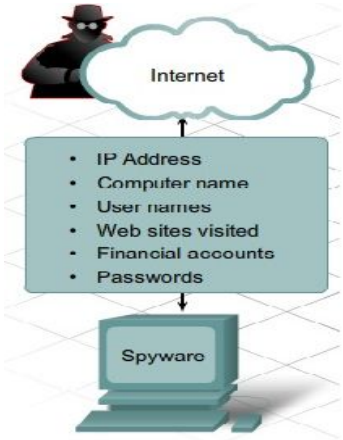
Distributed Denial of Service (DDoS)

- DDoS phức tạp và nguy cơ phá hại hơn DoS. Nó được thiết kế để tấn công tập trung và làm tràn ngập liên kết mạng.
- DDoS hoạt động ở phạm vi lớn hơn so với DoS. Thông thường hàng trăm hoặc hàng nghìn điểm tấn công cố gắng tấn công đích đồng thời.
- Các điểm tấn công này có thể là các máy tính không bị tình nghi mà đã bị lây nhiễm mã độc DDoS.



Spyware

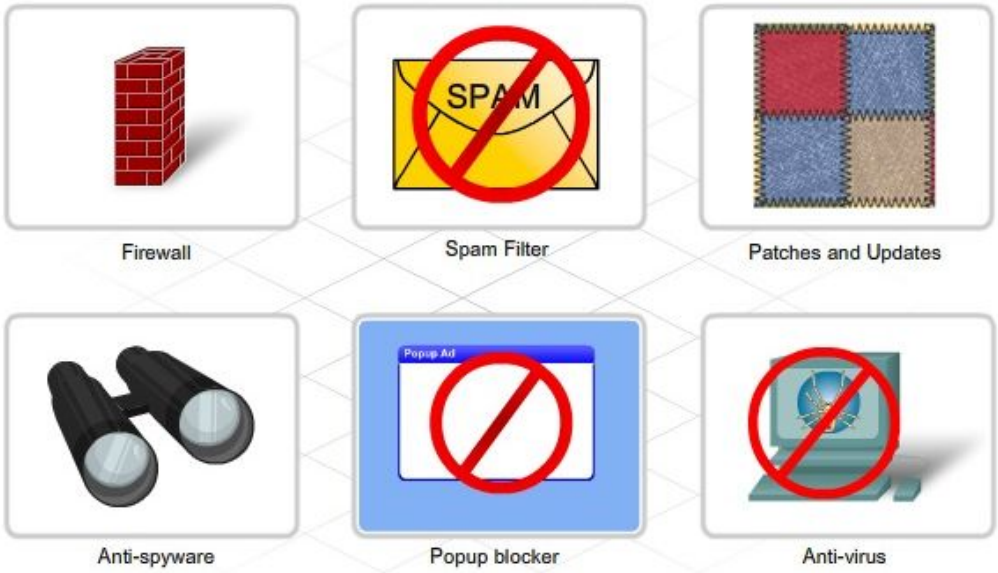
- Spyware là bất cứ chương trình mà thu nhận thông tin từ máy của bạn không cần sự cho phép và kiến thức của bạn. Thông tin này được gửi tới nhà quảng cáo hoặc đến người khác trên Internet và có thể bao gồm mật khẩu và số tài khoản.
- Spyware thông thường được cài khi bạn download 1 file, cài đặt một chương trình khác hoặc click vào popup. Nó có thể làm chậm máy tính và thay đổi các thiết lập bên trong việc này tạo ra khả năng dễ bị tấn công cho các mối hiểm họa khác.



Chính sách an ninh

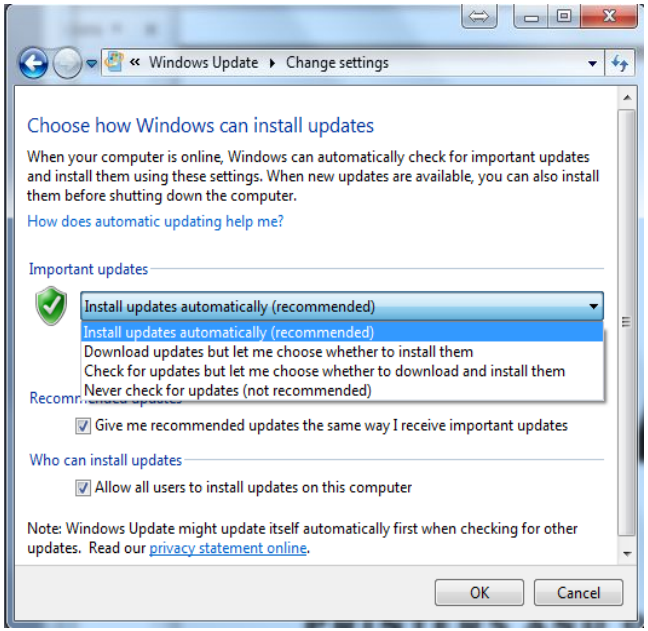
❖ Để hệ thống mạng đảm bảo an ninh phải sử dụng tổ hợp nhiều biện pháp:

- Cập nhật và vá lỗi các phần mềm.
- Sử dụng tường lửa (Firewall)
- Phần mềm quét virus.
- Phần mềm quét Spyware.
- Ngăn ngừa Spam /Pop-up



Cập nhật bản vá lỗi & update

- Một trong các phương pháp phổ biến mà hacker sử dụng để truy cập đến máy tính hoặc mạng là qua lỗ hổng của phần mềm.
- Quan trọng để giữ các phần mềm ứng dụng theo kịp các bản vá lỗi bảo mật và cập nhật để giúp ngăn cản hiểm họa.
- Patch là một đoạn code mà sửa lỗi cụ thể nào đó.

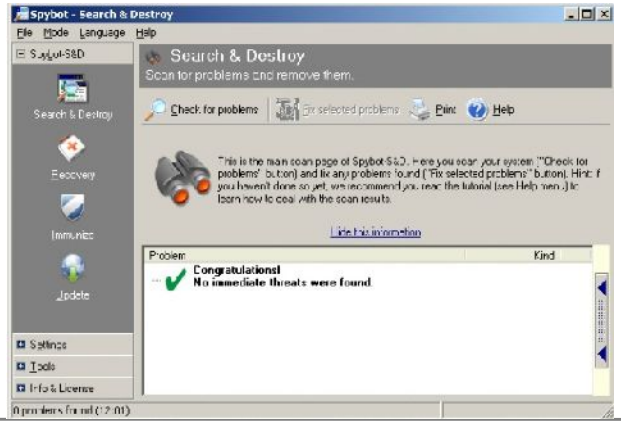


Phần mềm Anti-virus

- Phần mềm Anti-Virus có thể được sử dụng như cả hai tool ngăn ngừa và tool phản ứng lại virus. Nó ngăn cản sự lây nhiễm và phát hiện, và loại bỏ, virus, worms và Trojan Horses.
- Các đặc điểm bên trong phần mềm Anti-Virus là:
  - Kiểm tra Email: Quét cổng vào và cổng ra email, phát hiện các file kèm virus.
  - Quét thường trú động (Resident dynamic scanning): Kiểm tra các file thi hành và các tài liệu khi chúng được truy cập.
  - Lập lịch quét: Có thể lập lịch chạy ở một thời điểm và kiểm tra các ổ đĩa cứng hay toàn máy tính.
  - Tự động cập nhật: Kiểm tra, download và biết các mẫu virus.

Phần mềm Anti-Spyware

- Phần mềm gián điệp và phần mềm quảng cáo cũng có thể gây ra triệu chứng như là virus.
- Thêm vào đó chúng thu thập các thông tin không được quyền, Chúng có thể sử dụng các tài nguyên quan trọng của máy tính và ảnh hưởng đến hiệu năng hệ thống.
- Phần mềm Anti-Spyware phát hiện và xóa các ứng dụng gián điệp, cũng như ngăn cản việc cài đặt xảy ra trong tương lai. Nhiều phần mềm cũng phát hiện và xóa cookies và adware. Vài gói Anti-virus bao gồm chức năng anti-spyware.

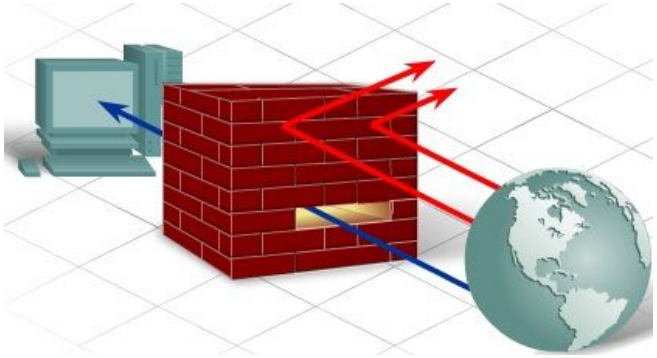


Sử dụng tường lửa (Firewall)

- Để bảo vệ các máy tính cá nhân và các Server gắn với mạng, quan trọng để kiểm soát các gói tin đến và ra khỏi mạng.
- Tường lửa là một phương pháp bảo mật hiệu quả nhất cho việc bảo vệ mạng bên trong từ các mối nguy hại từ bên ngoài. Tường lửa kiểm soát các gói tin giữa các mạng như là giúp ngăn cản truy cập bất hợp pháp. Các sản phẩm tường lửa sử dụng rất nhiều kỹ thuật khác nhau cho việc quyết định cái gì là được phép hoặc bị cấm truy cập đến mạng.
  - Lọc gói tin (Packet Filtering): Ngăn chặn hoặc cho phép truy cập dựa trên địa chỉ IP hoặc địa chỉ MAC.
  - Lọc ứng dụng (Application Filtering): Ngăn chặn hoặc cho phép truy cập các ứng dụng cụ thể dựa vào số hiệu cổng (Port Number).
  - Lọc URL (URL Filtering): Ngăn chặn hoặc cho phép truy cập Website dựa vào URL cụ thể hoặc từ khóa
  - Stateful Packet Inspection - SPI: Các gói tin đến phải được trả lời hợp lý tới các yêu cầu từ các host bên trong. Các gói tin không yêu cầu bị khóa ngoại trừ cho phép đặc biệt. SPI nhận dạng và loại bỏ tấn công như DoS.

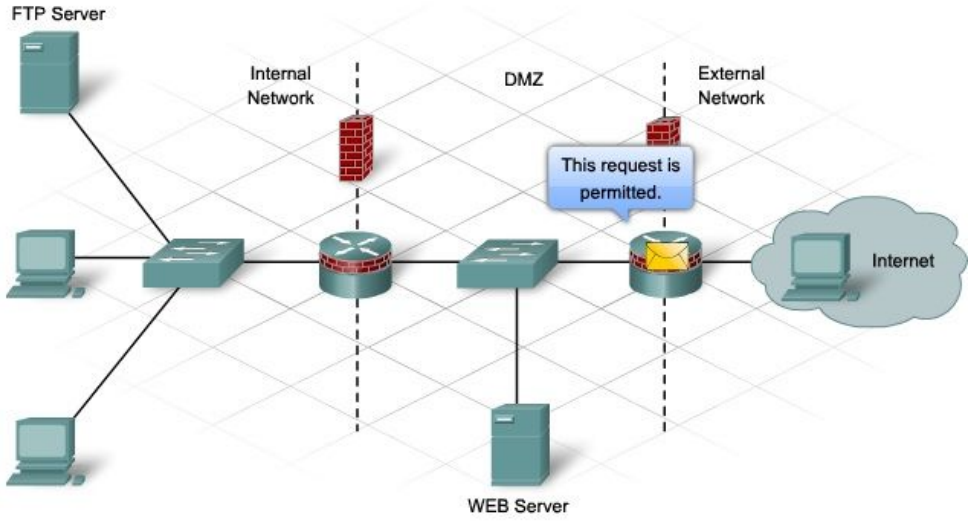
Sử dụng tường lửa

- Appliance-based firewalls: Là tường lửa được xây dựng tới 1 thiết bị chuyên nghiệp như là thiết bị an ninh.
- Server-based firewalls: bao gồm tường lửa ứng dụng mà chạy trên hệ điều hành mạng như là UNIX, Windows hoặc Novell.
- Integrated Firewalls – Được cài đặt bằng cách thêm các chức năng tường lửa đến các thiết bị đang tồn tại như là router.
- Personal firewalls: Nằm trên các máy tính và không được thiết kế cho LAN. Chúng có thể sẵn có mặc định từ hệ điều hành hoặc có thể cài đặt từ các hang khác.



Sử dụng tường lửa

- Bằng cách đặt tường lửa giữa mạng bên trong (intranet) và Internet như là thiết bị biên, tất cả các gói tin đến và từ Internet có thể bị giám sát và điều khiển.
- Điều này tạo nên môt đường phòng thủ giữa mạng bên trong và mạng bên ngoài.
- Tuy nhiên có thể có một vài khách hàng bên ngoài yêu cầu truy cập các tài nguyên bên trong.

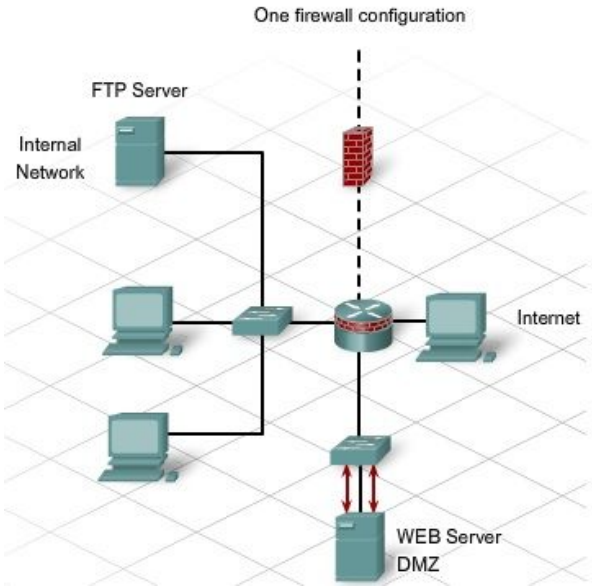


Sử dụng tường lửa

- Thuật ngữ DMZ (khu vực quân sự) được mượn từ quân sự. DMZ được thiết kế khu vực giữa hai quyền hạn ở đó các hoạt động của quân sự là không được phép.
- Trong mạng máy tính, DMZ tham chiếu tới một khu vực mạng mà nó có thể được truy cập tới cả hai người dùng bên trong và người dùng bên ngoài.
- Nó an toàn hơn mạng bên ngoài nhưng không an toàn như mạng bên trong.
- Nó được tạo bởi một hoặc nhiều tường lửa để phân tách bên trong, DMZ và các mạng bên ngoài.
- Các Web server cho truy cập public thường xuyên đặt tại DMZ.

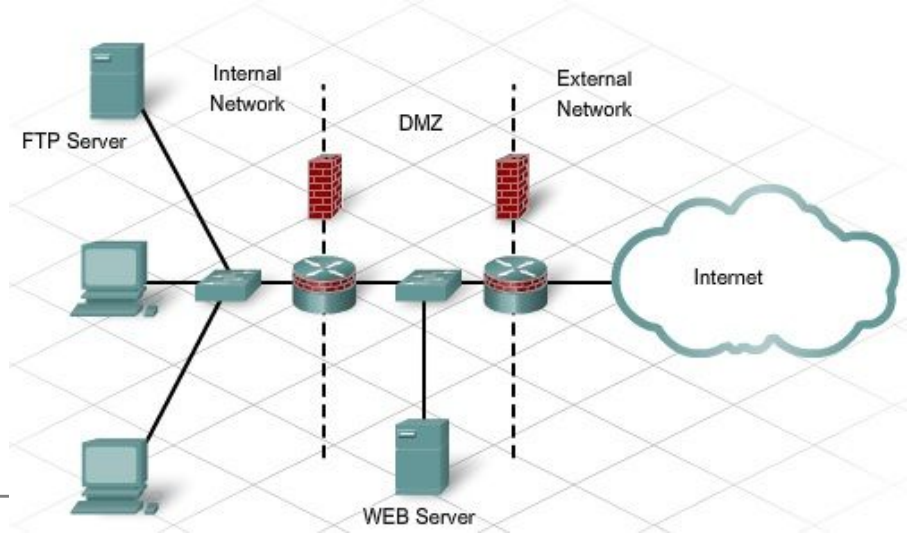
Cấu hình một tường lửa

- Một tường lửa đơn có 3 khu vực, một cho mạng bên ngoài, một cho mạng bên trong và DMZ.
- Tất cả các gói tin được gửi từ mạng bên ngoài đến Firewall. FW được yêu cầu để giám sát gói tin và quyết định xem những gói tin nào được chuyển tới DMZ, gói tin nào được chuyển tới mạng bên trong, gói tin nào bị từ chối hoàn toàn.



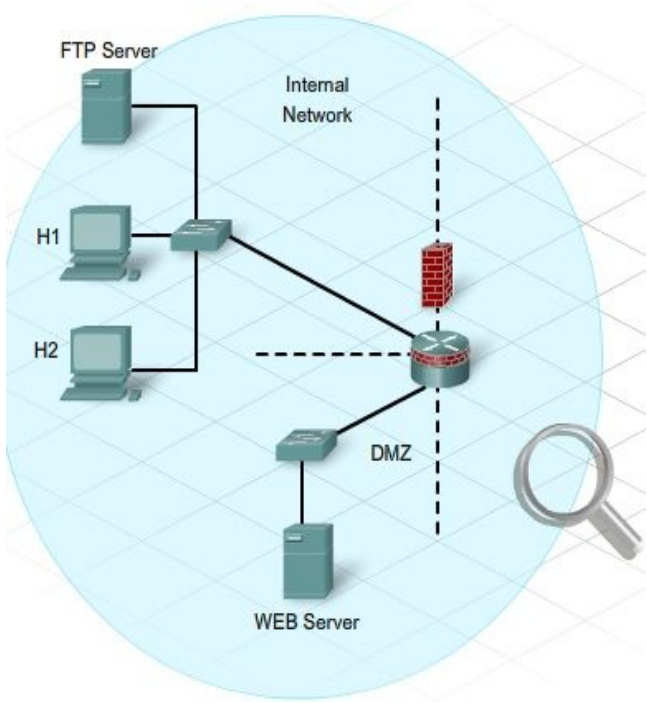
Cấu hình hai tường lửa

- Trong cấu hình hai tường lửa, có một tường lửa bên trong và có tường lửa bên ngoài với DMZ đặt giữa chúng.
- Tường lửa bên ngoài là ít hạn chế và cho phép các người dùng Internet truy cập các dịch vụ tới DMZ như là cho phép gói tin mà bất cứ người dùng bên trong yêu cầu chuyển qua. Tường lửa bên trong hạn chế và bảo vệ mạng bên trong tốt hơn từ các truy cập trái phép.
- Thích hợp hơn cho mạng lớn, phức tạp điều khiển nhiều gói tin hơn.



Phân tích điểm yếu hệ thống mạng

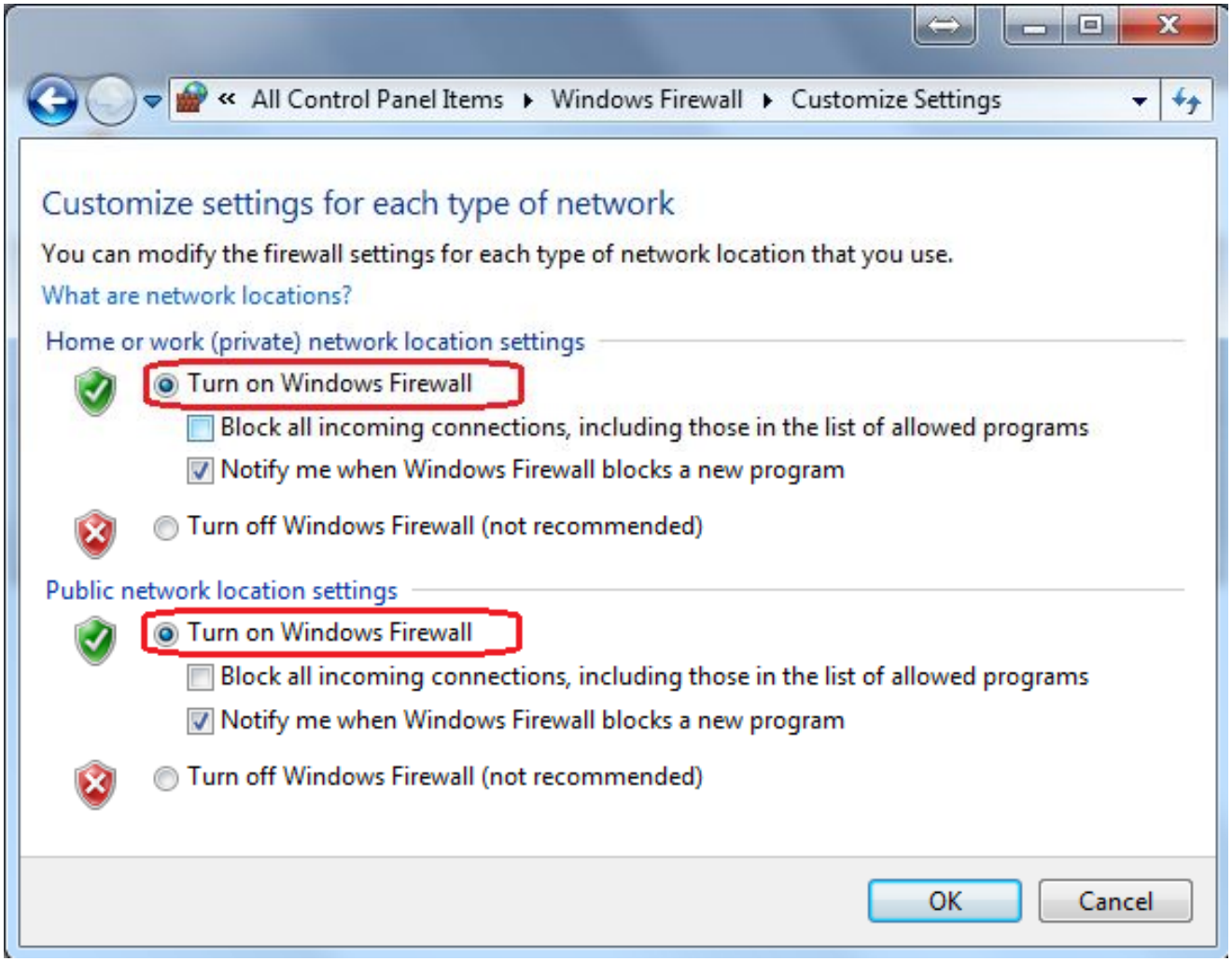
- Có rất nhiều công cụ phân tích điểm yếu cho máy và an ninh mạng. Đó là các phần mềm quét an toàn, và có thể giúp ta xác định khu vực mà có thể xảy ra tấn công và cung cấp các hướng dẫn.
- Một số đặc trưng:
  - Số máy trên mạng.
  - Các dịch vụ mạng đang cung cấp.
  - Hệ điều hành và phiên bản của host.
  - Lọc các gói tin và tường lửa được sử dụng.



Tường lửa cá nhân Windows

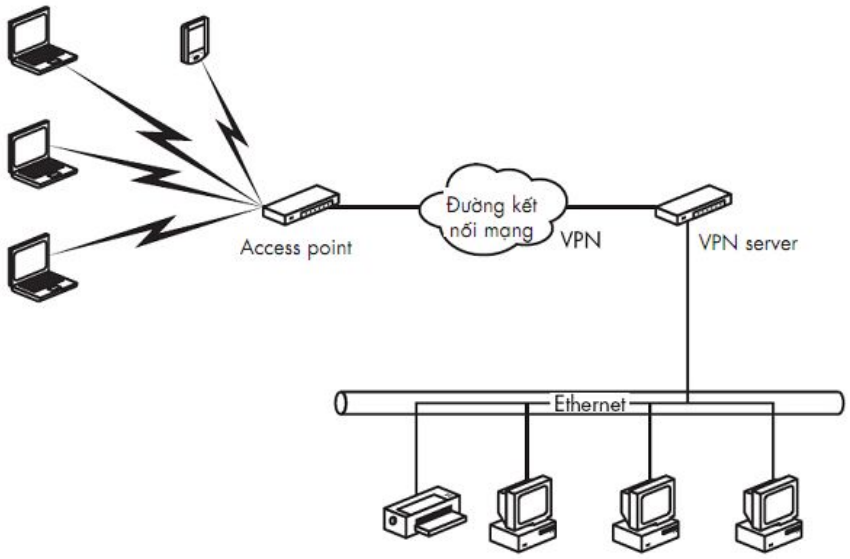
- Tường lửa là một chức năng ngăn chặn những truy nhập trái phép vào hệ thống máy tính của bạn thông qua việc lọc bỏ những địa chỉ không hợp lệ. Tường lửa thường được đặt tại cổng ra vào giữa hai hệ thống mạng như từ mạng LAN này tới mạng LAN khác hoặc từ máy tính tới Internet.
- Để thiết lập tường lửa vào Start gõ firewall trong ô tìm kiếm, bạn sẽ thấy kết quả hiển thị các mục liên quan đến firewall, chọn mục Windows Firewall, trong cửa sổ firewall chọn mục Turn Windows Firewall on or off và chọn Turn on...

Tường lửa cá nhân Windows



Tường lửa

- Ngoài chức năng có sẵn của Windows, bạn có thể sử dụng các phần mềm khác có chức năng firewall hoặc những thiết bị phần cứng có chức năng firewall như bộ Access Point phát sóng không dây
- Ngoài ra bạn có thể thiết lập một mạng riêng ảo (Virtual Private Network) để trao đổi dữ liệu an toàn hơn



Hình 13-4: VPN cung cấp một kết nối bảo mật giữa mạng không dây và gateway Internet hoặc một mạng LAN.

❖ Để thiết lập bảo mật cho mạng không dây, bạn phải đăng nhập vào thiết bị và cấu hình với những chế độ sau:

Chế độ	Ý nghĩa
WEP	Khóa cố định, độ dài mã hóa 64, 128, 152 bit
WPA/WPA-PSK	Mã hóa cao hơn WEP, khóa thay đổi dùng cho doanh nghiệp hoặc gia đình
WPA2/WPA2-PSK	Sử dụng chuẩn mã hóa cao cấp hơn WPA, khóa thay đổi có thể dùng cho doanh nghiệp hoặc gia đình
Mixed WPA2/WPA	Dùng cho doanh nghiệp, có hai chế độ
Mixed WPA2/WPA-PSK	Dùng cho gia đình, có hai chế độ

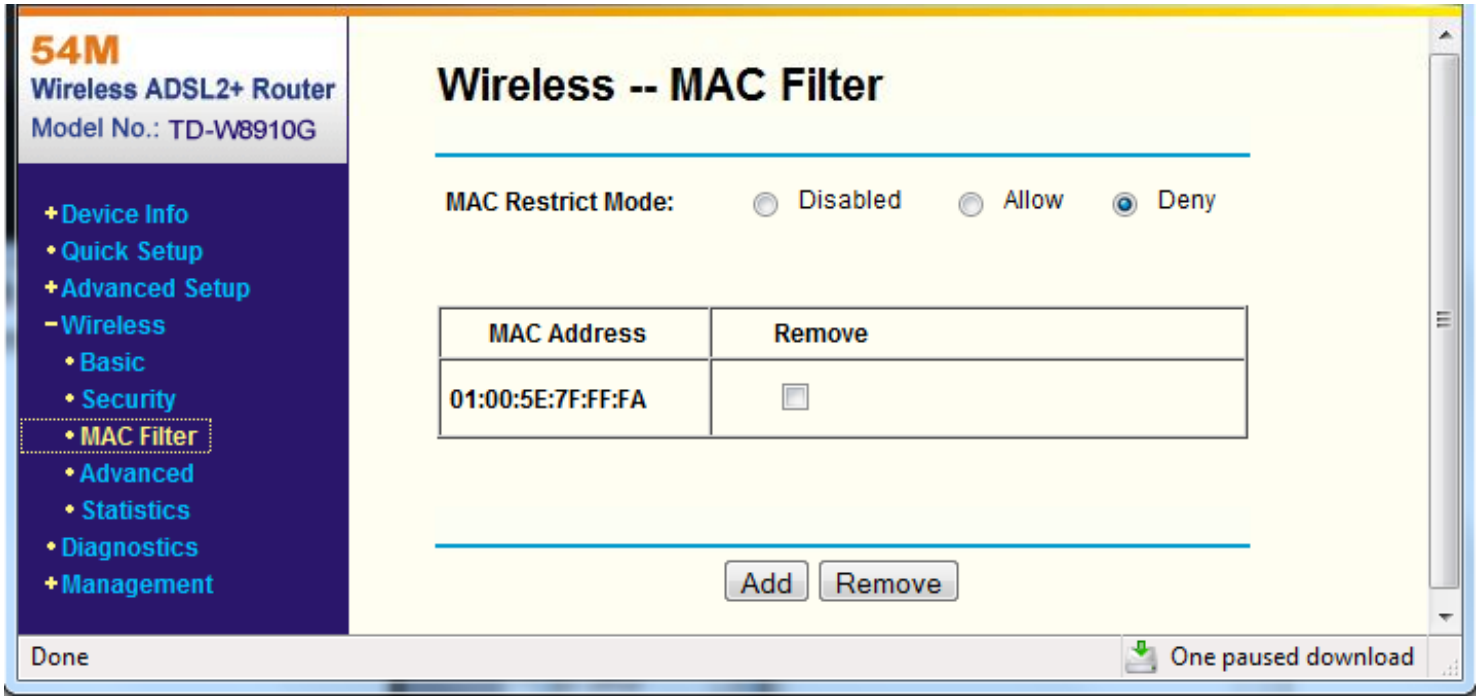
Bảo mật mạng không dây

- Ở chế độ WEP, bạn phải nhập mật khẩu với độ dài tương ứng
  - 5 ký tự hoặc 10 số cho mã hóa 64 bit
  - 13 ký tự hoặc 26 số cho mã hóa 128 bit
  - 16 ký tự hoặc 32 số cho mã hóa 152 bit

- Ở các chế độ khác, độ dài mật khẩu là không bắt buộc

Địa chỉ MAC

- Mỗi thiết bị điện tử có một địa chỉ duy nhất để phân biệt gọi là địa chỉ MAC. Trong bộ Access point thường hỗ trợ cho phép/chặn địa chỉ MAC của thiết bị đăng nhập vào hệ thống. Bạn có thể sử dụng chức năng này để chặn những thiết bị không mong muốn bằng chức năng MAC Filter.



Tổng kết – Câu hỏi

- Mục đích của việc tạo tài khoản người dùng với những quyền khác nhau?
- Tại sao phải dùng tường lửa? Những hệ thống nào có hỗ trợ tường lửa? Bạn biết gì về phần mềm Zone Alarm?
- Tại sao thường xuyên update hệ điều hành là một việc nên làm?
- Bảo mật sóng Wi-Fi có những kiểu mã hóa nào? Hiện nay kiểu mã hóa nào là an toàn nhất? Tại sao?
- Phân biệt kiểu mã hóa sử dụng chức năng RADIUS và chức năng PSK (Pre-Shared Key)?