Học viện kỹ thuật quân sự

Khoa công nghệ thông tin

**Báo cáo đảm bảo an toàn thông tin**

**Đề tài:** Khả năng bảo vệ hệ thống của trình quét virus và firewall

**Giáo viên hướng dẫn:** Nguyễn Văn Quân

**Nhóm 11:** Vũ Đức Hoàng

Vũ Hữu Nghĩa

Đỗ Văn Mạnh

Đỗ Hữu Tuyến

Hà Nội 2016

**Mục lục**

[Phần một: Giới thiệu chung về vấn đề 3](#_Toc463960272)

[Phần hai: Nội dung 4](#_Toc463960273)

[**I.** **Trình quét virus** 4](#_Toc463960274)

[1. Virus 4](#_Toc463960275)

[2. Trình quét virus 6](#_Toc463960276)

[*a.* *Khái niệm* 6](#_Toc463960277)

[*b.* *Các kỹ thuật phát hiện, diệt virus* 6](#_Toc463960278)

[*c.* *Khả năng bảo vệ và hạn chế* 9](#_Toc463960279)

**II. Firewall**

[1. Thế nào là firewall 12](#_Toc463960280)

[2. Nhiệm vụ firewall 12](#_Toc463960281)

[3. Phân loại firewall 12](#_Toc463960282)

[4. Nguyên lý hoạt động của firewall 13](#_Toc463960283)

[5. Chức năng của firewall 14](#_Toc463960284)

[6. Ưu, nhược điểm của firewall 14](#_Toc463960285)

[Phần Ba: Kết luận 17](#_Toc463960286)

# Phần một: Giới thiệu chung về vấn đề

# Phần hai: Nội dung

1. **Trình quét virus**
2. Virus

Trong [khoa học máy tính](https://vi.wikipedia.org/wiki/Khoa_h%E1%BB%8Dc_m%C3%A1y_t%C3%ADnh), **virus máy tính** (thường được người sử dụng gọi tắt là virus hay **vi-rút**) là những [chương trình](https://vi.wikipedia.org/wiki/Ch%C6%B0%C6%A1ng_tr%C3%ACnh) hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó tạo ra những tệp tin (file) bị nhiễm virus trên các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là usb),...

Virus hiểu theo nghĩa rộng không chỉ bao gồm virus máy tính nói riêng mà bao gồm tất cả phần mềm, chương trình, đoạn mã có thể gây hại cho máy tính.

* [**Phần mềm ác tính**](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_%C3%A1c_%C3%BD) (*malware*) chỉ chung các [phần mềm](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m) có tính năng gây hại như virus, worm và Trojan horse...
* [**Sâu máy tính**](https://vi.wikipedia.org/wiki/S%C3%A2u_m%C3%A1y_t%C3%ADnh) (*worm*): Là các chương trình cũng có khả năng tự nhân bản tự tìm cách lan truyền qua hệ thống [mạng](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng) (thường là qua hệ thống thư điện tử). Điểm cần lưu ý ở đây, ngoài gây tác hại cho máy bị nhiễm, nhiệm vụ chính của worm là phá các mạng (*network*) thông tin chia sẻ, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này. Nhiều nhà phân tích cho rằng worm khác với virus, họ nhấn mạnh vào đặc tính phá hoại mạng nhưng ở đây worm được là một loại virus đặc biệt.
* [**Trojan Horse**](https://vi.wikipedia.org/wiki/Trojan): Đây là loại chương trình cũng có tác hại tương tự như virus chỉ khác là nó không tự nhân bản ra. Như thế, cách lan truyền duy nhất là thông qua các thư dây chuyền. Để trừ loại này người chủ máy chỉ việc tìm ra tập tin Trojan horse rồi xóa nó đi là xong. Tuy nhiên, không có nghĩa là không thể có hai con Trojan horse trên cùng một hệ thống. Chính những kẻ tạo ra các phần mềm này sẽ sử dụng kỹ năng lập trình của mình để sao lưu thật nhiều con trước khi phát tán lên mạng. Đây cũng là loại virus cực kỳ nguy hiểm. Nó có thể hủy ổ cứng, hủy dữ liệu.
* [**Phần mềm gián điệp**](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_gi%C3%A1n_%C4%91i%E1%BB%87p) (*spyware*): Đây là loại virus có khả năng thâm nhập trực tiếp vào [hệ điều hành](https://vi.wikipedia.org/wiki/H%E1%BB%87_%C4%91i%E1%BB%81u_h%C3%A0nh) mà không để lại "di chứng". Thường một số chương trình diệt virus có kèm trình diệt spyware nhưng diệt khá kém đối với các đợt "dịch".
* [**Phần mềm quảng cáo**](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_qu%E1%BA%A3ng_c%C3%A1o) (*adware*): Loại phần mềm quảng cáo, rất hay có ở trong các chương trình cài đặt tải từ trên mạng. Một số phần mềm vô hại, nhưng một số có khả năng hiển thị thông tin kịt màn hình, cưỡng chế người sử dụng.
* [**Botnet**](https://vi.wikipedia.org/wiki/Botnet): Là những máy tính bị bắt cóc và điều khiển bởi người khác thông qua Trojan, virus...Điều đặc biệt nguy hiểm là các botnet được phơi bày từ các tin tặc không cần kỹ thuật lập trình cao. Nó được rao bán với giá từ 20USD trở lên cho các tin tặc. Hậu quả của nó để lại không nhỏ: mất tài khoản. Nếu liên kết với một hệ thống máy tính lớn, nó có thể tống tiền cả một doanh nghiệp.
* [**Keylogger**](https://vi.wikipedia.org/wiki/Keylogger): Là phần mềm ghi lại chuỗi phím gõ của người dùng. Nó có thể hữu ích cho việc tìm nguồn gốc lỗi sai trong các hệ thống máy tính và đôi khi được dùng để đo năng suất làm việc của nhân viên văn phòng. Các phần mềm kiểu này rất hữu dụng cho ngành luật pháp và tình báo - ví dụ, cung cấp một phương tiện để lấy mật khẩu hoặc các khóa mật mã và nhờ đó qua mắt được các thiết bị an ninh. Tuy nhiên, các phần mềm keylogger được phổ biến rộng rãi trên Internet và bất cứ ai cũng có thể sử dụng cho mục đích lấy trộm mật khẩu và chìa khóa mã hóa.
* [**Phishing**](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_gi%E1%BA%A3_m%E1%BA%A1o): Là một hoạt động phạm tội dùng các kỹ thuật lừa đảo. Kẻ lừa đảo cố gắng lừa lấy các thông tin nhạy cảm, chẳng hạn như mật khẩu và thông tin về [thẻ tín dụng](https://vi.wikipedia.org/wiki/Th%E1%BA%BB_t%C3%ADn_d%E1%BB%A5ng), bằng cách giả là một người hoặc một doanh nghiệp đáng tin cậy trong một giao dịch điện tử. Phishing thường được thực hiện bằng cách sử dụng thư điện tử hoặc tin nhắn, đôi khi còn sử dụng cả điện thoại.
* [**Rootkit**](https://vi.wikipedia.org/wiki/Rootkit): Là một bộ công cụ phần mềm dành cho việc che giấu các tiến trình đang chạy, các file hoặc dữ liệu hệ thống. Rootkit có nguồn gốc từ các ứng dụng tương đối hiền, nhưng những năm gần đây, rootkit đã bị sử dụng ngày càng nhiều bởi các phần mềm ác tính, giúp kẻ xâm nhập hệ thống giữ được đường truy nhập một hệ thống trong khi tránh bị phát hiện. Người ta đã biết đến các rootkit dành cho nhiều hệ điều hành khác nhau chẳng hạn [Linux](https://vi.wikipedia.org/wiki/Linux),
* [**Solaris**](https://vi.wikipedia.org/wiki/Solaris) và một số phiên bản của [Microsoft Windows](https://vi.wikipedia.org/wiki/Microsoft_Windows). Các rootkit thường sửa đổi một số phần của hệ điều hành hoặc tự cài đặt chúng thành các [driver](https://vi.wikipedia.org/wiki/Driver) hay các môdule trong [nhân hệ điều hành](https://vi.wikipedia.org/wiki/Nh%C3%A2n_h%E1%BB%87_%C4%91i%E1%BB%81u_h%C3%A0nh) (*kernel module*).
* [**Phần mềm tống tiền**](https://vi.wikipedia.org/w/index.php?title=Ph%E1%BA%A7n_m%E1%BB%81m_t%E1%BB%91ng_ti%E1%BB%81n&action=edit&redlink=1) (*Ransomware*): Là loại phần mềm sử dụng một hệ thống mật mã để mã hóa dữ liệu thuộc về một cá nhân và đòi tiền chuộc thì mới khôi phục lại.
* [**Backdoor**](https://vi.wikipedia.org/wiki/Backdoor): Backdoor, nghĩa là "cửa hậu" hay lối vào phía sau. Trong một hệ thống máy tính, "cửa hậu" là một phương pháp vượt qua thủ tục chứng thực người dùng thông thường hoặc để giữ đường truy nhập từ xa tới một máy tính, trong khi cố gắng không bị phát hiện bởi việc giám sát thông thường. Cửa hậu có thể có hình thức một chương trình được cài đặt (ví dụ Back Orifice hoặc cửa hậu rookit Sony/BMG rootkit được cài đặt khi một đĩa bất kỳ trong số hàng triệu đĩa CD nhạc của Sony được chơi trên một máy tính chạy Windows), hoặc có thể là một sửa đổi đối với một chương trình hợp pháp - đó là khi nó đi kèm với Trojan.

1. Trình quét virus
2. *Khái niệm*

**Phần mềm diệt virus** là [phần mềm](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m) có tính năng phát hiện, loại bỏ các [virus máy tính](https://vi.wikipedia.org/wiki/Virus_(m%C3%A1y_t%C3%ADnh)), khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus trong tương lai.

Để đạt được các mục tiêu tối thiểu trên và mở rộng tính năng, phần mềm diệt virus thường hoạt động trên các nguyên lí cơ bản nhất như sau:

* Kiểm tra (quét) các [tập tin](https://vi.wikipedia.org/wiki/T%E1%BA%ADp_tin) để phát hiện các virus đã biết trong cơ sở dữ liệu nhận dạng về virus của chúng.
* Phát hiện các hành động của các phần mềm giống như các hành động của virus hoặc các phần mềm độc hại.

1. *Các kỹ thuật phát hiện, diệt virus*

* So sánh với mẫu virus biết trước

Toàn bộ các phần mềm diệt virus đều sử dụng kỹ thuật này để quét virus. Kỹ thuật so sánh với mẫu có thể mô tả đơn giản như sau: Các file cần kiểm tra virus được phân tích và so sánh với các mẫu virus đã biết trước, nếu phát hiện một đoạn mã virus thì file đó có thể bị lây nhiễm virus và phần mềm thực hiện biện pháp loại bỏ virus khỏi file bị lây nhiễm. Tất nhiên đây là việc mô tả đơn giản, các hành động cụ thể của các phần mềm này phức tạp hơn nhiều để có thể quét nhanh nhất, loại bỏ sự nhầm lẫn và việc sửa chữa file không làm hư hỏng file.

Kỹ thuật so sánh mẫu virus khiến cho các phần mềm liên tục phải cập nhật cơ sở dữ liệu để có khả năng nhận biết các loại virus mới cùng các biến thể của nó.

### Đám mây antivirus

Đám mây antivirus là một công nghệ có sử dụng phần mềm đại lý nhẹ trên máy tính được bảo vệ, trong khi bán ra phần lớn các phân tích dữ liệu cơ sở hạ tầng của nhà cung cấp.

Một cách tiếp cận để triển khai điện toán đám mây chống virus liên quan đến chức năng quét tập tin nghi ngờ sử dụng nhiều công cụ chống virus. Cách tiếp cận này đã được đề xuất bởi một thực hiện đầu của khái niệm đám mây chống virus được gọi là CloudAV. CloudAV được thiết kế để gửi các chương trình hoặc tài liệu để một [đám mây mạng](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Cloud_computing&usg=ALkJrhgRIoZpAOZm1NQOtmghe73ta-IJIg) mà nhiều virus và các chương trình phát hiện hành vi được sử dụng đồng thời để nâng cao tỷ lệ phát hiện. Quét song song các file sử dụng máy quét chống virus có khả năng không tương thích được thực hiện bằng cách đẻ trứng một máy ảo trên mỗi công cụ phát hiện và do đó loại bỏ bất kỳ vấn đề có thể. CloudAV cũng có thể thực hiện "phát hiện hồi tố", theo đó các công cụ phát hiện đám mây quét lại tất cả các file trong lịch sử truy cập tập tin của nó khi một mối đe dọa mới được xác định do đó cải thiện tốc độ phát hiện mối đe dọa mới. Cuối cùng, CloudAV là một giải pháp cho việc quét virus hiệu quả trên các thiết bị thiếu sức mạnh tính toán để thực hiện việc quét tự.

Như ta đã biết về virus với cơ chế lây nhiễm của nó vào các file: Chúng gắn chính đoạn mã của bản thân vào một phần của file để được kích hoạt khi thực thi file này. Kỹ thuật so sánh mẫu sẽ phát hiện ra các đoạn mã của virus giống như dấu hiệu nhận biết trong cơ sở dữ liệu của phần mềm diệt virus, phần mềm sẽ tiến hành loại bỏ các đoạn mã này. Quá trình này có thể xảy ra các vấn đề:

* Để đảm bảo các phần cập nhật có dung lượng không quá lớn, cơ sở dữ liệu có thể được lược giản, do đó khi sửa chữa file bị lây nhiễm có thể chỉ xóa một đoạn mã đặc trưng, quan trọng nên có thể phần mềm khác (với cơ chế so sánh ở một đặc điểm khác) có thể vẫn phát hiện file đó bị nhiễm virus.
* Việc xóa các đoạn mã được coi là của một virus nào đó có thể dẫn đến phần mềm vô tình xóa đoạn mã nhận dạng ở một file hoàn toàn không bị lây nhiễm virus: Đây là hiện tượng nhận nhầm không thể tránh khỏi bởi người viết phần mềm không thể lường hết mọi file của mọi phần mềm trên thến giới, tuy nhiên cần hạn chế đến mức tối thiểu và phải được sửa đổi ngay khi phát hiện ra sự nhầm lẫn.
* Nhiều file được gắn các "chữ ký điện tử" nhằm xác nhận file có nguồn gốc, đảm bảo an toàn, sau khi bị lây nhiễm virus và được diệt bởi một phần mềm diệt virus, file có thể không còn chữ ký, do đó cần thay thế file đó bằng file nguyên bản hoặc cài đặt lại phần mềm.
* Việc sửa chữa file đã bị nhiễm virus cũng có thể còn gây nên hư hỏng file nên các phần mềm diệt virus thường lưu lại file trước khi sửa chữa (vẫn nguyên tình trạng bị nhiễm virus) dưới dạng nén lại hoặc mã hóa để không thể lây nhiễm ngược trở lại. Ở đây có thể cần hai trường hợp: Nếu phần mềm diệt virus được cập nhật các thuật toán mới (nâng cấp engine) thì nên phục hồi để diệt lại; Nếu hệ điều hành hoặc các phần mềm khác bị nhiễm quá nhiều thể loại virus mà đã được diệt nhưng hệ thống không ổn định thì nên cài đặt lại hệ điều hành (hoặc phần mềm) để có được các file nguyên ban
* Nhận dạng hành vi đáng ngờ

Nhận dạng các hành vi đáng ngờ là một chức năng "thông minh" mà không phải bất kỳ phần mềm diệt virus nào cũng có. Hiểu một cách đơn giản thì phần mềm diệt virus sẽ theo dõi sự hoạt động bất thường của hệ thống để có thể phát hiện các virus chưa được biết đến (trong dữ liệu của nó) hoặc các phần mềm độc hại để từ đó đưa ra cảnh báo người sử dụng, cô lập virus để sẵn sàng gửi mẫu đến hãng bảo mật phân tích và cập nhật vào bản nâng cấp cơ sở dữ liệu kế tiếp.

Chức năng này ở các phần mềm diệt virus thường cho phép lựa chọn kích hoạt hoặc không, mức độ hoạt động (sử dụng ở mức độ hoạt động tích cực, hoạt động trung bình ở mức đề cử, hay hoạt động ở mức độ thấp - mặc định thiết lập thường là kích hoạt sẵn ở mức độ đề cử) bởi đa số chúng có thể chiếm tài nguyên và làm chậm hệ thống đối với các máy tính không đủ mạnh.

* Kiểm soát liên tục

Phần mềm diệt virus máy tính thường thực hiện kiểm soát liên tục theo thời gian thực để bảo vệ hệ thống. Hình thức kiểm soát liên tục sẽ quét virus mọi file mà hệ thống truy cập đến, mọi file ngay từ khi bắt đầu được copy vào hệ thống thông qua hình thức nhận biết so sánh mẫu và theo dõi hành động đáng ngờ.

* Kết hợp mọi phương thức

Nếu chỉ đơn thuần sử dụng kỹ thuật so sánh mẫu thì một phần mềm diệt virus sẽ thất bại bởi chúng chỉ giải quyết hậu quả các file bị nhiễm chứ chưa tìm đến nguyên nhân dẫn đến file bị nhiễm. Khi sử dụng một số phần mềm chưa đủ mạnh bạn sẽ nhận thấy trường hợp: Phần mềm đã diệt được hoàn toàn virus trong máy, nhưng ngay sau khi phiên khởi động kế tiếp của hệ điều hành, phần mềm lại phát hiện ra virus chính virus đó. Đây có thể không phải là phần mềm nhận dạng được nhưng không diệt được, mà là virus lại được lây nhiễm trở lại bởi phần mềm đã không thể giám sát quá trình khởi động hệ điều hành ngay từ khi bios trao quyền điều khiển.

Chính vì vậy, phần mềm cần phải kết hợp mọi phương thức để kiểm soát và ngăn chặn các hành vi của virus. Virus có thể đặt các dòng lệnh trong registry để lây nhiễm virus từ một file nén nào đó hoặc vô hiệu hóa phần mềm diệt virus; Cũng có thể virus thiết lập tải về ngay khi sử dụng trình duyệt để kết nối vào mạng Internet. Do vậy phần mềm diệt virus cần phải kết hợp mọi phương thức để ngăn chặn virus. Chính những yếu tố này làm lên sự khác biệt giữa các phần mềm diệt virus hiện nay, không lẫn nó với vô vàn phần mềm diệt virus khác khi mà ngay một sinh viên cũng có thể viết một phần mềm diệt virus nếu chịu khó sưu tầm các mẫu virus trên mạng Internet hiện nay.

1. *Khả năng bảo vệ và hạn chế*

* **Hiệu quả**

Các trình quét virus bảo vệ máy tính khỏi các mối đe dọa:

* Viruses, Trojans, sâu máy tính và các chương trình độc hại khác, Spyware và Adware Rootkits, Bootkits và các mối đe dọa khác
* Đánh cắp mã số cá nhân với các chương trình Keyloggers, chụp màn hình hoặc lừa đảo
* Dùng Botnets và các phương pháp lừa đảo khác để chiếm quyền điều khiển máy tính của bạn
* Tấn công Zero-day, và những mối nguy hiểm chưa xác định được
* Tải về các trình điều khiển độc hại, tấn công mạng
* Các website độc hại và thư rác
* Giữ an toàn cho tài khoản và dữ liệu cá nhân của bạn
* Bảo vệ bạn chống lại việc đánh cắp tài khoảng ngân hàng
* Giữ bạn an toàn khi thực hiện mua bán trực tuyến
* Cho phép các ứng dụng và website khả nghi
* Chạy trong ””Chế độ an toàn””
* Tội phạm công nghệ không thể kiểm soát máy tính của bạn
* Bảo vệ gia đình khỏi các nguy hiểm trên internet
* Các tập tin của bạn không thể bị đánh cắp bởi hacker
* Giữ máy tính của bạn chạy ổn định
* Giữ các kết nối Wi-Fi an toàn
* Hai lớp tường lửa cá nhân
* **Hạn chế**
* Phần mềm diệt virus có một số nhược điểm, như nó có thể ảnh hưởng đến một hiệu suất máy tính.
* Hơn nữa, người dùng không có kinh nghiệm có thể được ru ngủ trong một cảm giác sai lầm về bảo mật khi sử dụng máy tính, xem xét mình là bất khả xâm phạm, và có thể có vấn đề hiểu biết các hướng dẫn và quyết định rằng phần mềm chống virus trình bày chúng với.Một quyết định sai có thể dẫn đến vi phạm an ninh. Nếu phần mềm diệt virus sử dụng phát hiện heuristic, nó phải được điều chỉnh để giảm thiểu misidentifying phần mềm vô hại như độc hại ([false positive](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/False_positive&usg=ALkJrhiw0IkqGmQhhTVhXWirZ0wXw9zQ-g)).
* Phần mềm diệt virus bản thân thường chạy vào cấp độ tin cậy cao của [hệ điều hành](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Operating_system&usg=ALkJrhgHhug2etl_KwNBdNyehWt9LpVGNw) để cho phép nó truy cập vào tất cả các quá trình độc hại tiềm năng và các tập tin, tạo ra một con đường tiềm năng của [cuộc tấn công](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Attack_(computing)&usg=ALkJrhg0oH60ObEHF6F0kAiysFGQeN6JQg) .
* Cài đặt các giải pháp chống virus, chạy trên các máy tính cá nhân, mặc dù sử dụng nhiều nhất, chỉ có một phương pháp bảo vệ chống lại phần mềm độc hại. Các giải pháp thay thế khác cũng được sử dụng, bao gồm: [Unified Threat Management](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Unified_Threat_Management&usg=ALkJrhjjZLQ-mty66h0MDo2PWMY8154scg) ( [UTM](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Unified_Threat_Management&usg=ALkJrhjjZLQ-mty66h0MDo2PWMY8154scg) ), phần cứng và mạng tường lửa, [dựa trên đám mây](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Cloud_computing&usg=ALkJrhgRIoZpAOZm1NQOtmghe73ta-IJIg) chống virus và máy quét trên mạng.
* **Vi-rút mới**
* các chương trình chống virus không phải luôn luôn hiệu quả chống lại các loại virus, ngay cả những người sử dụng phương pháp không dựa trên chữ ký mà nên phát hiện virus mới. Lý do cho điều này là các nhà thiết kế vi rút thử nghiệm virus mới của họ trên các ứng dụng chống virus lớn để đảm bảo rằng họ không được phát hiện trước khi thả chúng vào tự nhiên. [[130]](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Antivirus_software&usg=ALkJrhhn4npTN4_sTe3XAYY61zMA0_XGhQ#cite_note-130)
* Một số virus mới, đặc biệt [ransomware](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Ransomware_(malware)&usg=ALkJrhhy8lQ6xgiew2BRGdRePIgBLk5Uig) , sử dụng [đang đa hình](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Polymorphic_code&usg=ALkJrhigK3Wrd5XStpUPUCBiyejcaV1A0g) để tránh bị phát hiện bởi máy quét virus.
* Một [bằng chứng của khái niệm](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Proof_of_concept&usg=ALkJrhiLlhSjiXXy20-fSE34ciDHyne8Vw) virus đã sử dụng các [đơn vị xử lý đồ họa](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Graphics_Processing_Unit&usg=ALkJrhjehpX-9WYITRvwywdial3iLIZ2GQ) (GPU) để tránh bị phát hiện từ phần mềm chống virus. Sự thành công tiềm năng của việc này liên quan đến việc bỏ qua các [CPU](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Central_processing_unit&usg=ALkJrhggcBDU1iXzdiZO-AK0UVXPTm6e7w) để làm cho nó khó khăn hơn nhiều cho các nhà nghiên cứu an ninh để phân tích các hoạt động bên trong của phần mềm độc hại như vậy.
* **Rootkits**
* Phát hiện [rootkit](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Rootkit&usg=ALkJrhhRL46LoB84uP92NWEZFqR_qoJgNQ) là một thách thức lớn đối với các chương trình chống virus. Rootkit có đầy đủ quyền truy cập quản trị vào máy tính và được ẩn với người dùng và ẩn từ danh sách các tiến trình đang chạy trong [công việc quản lý](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Task_manager&usg=ALkJrhgZHU08rayDStn7b_ejebcQSWz16g) . Rootkit có thể sửa đổi các hoạt động bên trong của [hệ điều hành](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Operating_system&usg=ALkJrhgHhug2etl_KwNBdNyehWt9LpVGNw) và làm xáo trộn với các chương trình chống virus.
* **File bị hỏng**
* Nếu một tập tin đã bị nhiễm bởi một loại virus máy tính, phần mềm chống virus sẽ cố gắng để loại bỏ các mã virus từ các tập tin trong khử trùng, nhưng nó không phải là luôn luôn có thể khôi phục lại các tập tin vào nhà nước không bị hư hại của nó.Trong hoàn cảnh như vậy, các file bị hỏng chỉ có thể được khôi phục từ bản sao lưu hiện có hoặc [bản sao bóng tối](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Shadow_copy&usg=ALkJrhjtbILpywBiRRg92Vl9_Os2laxqOA) (điều này cũng đúng đối với ransomware); phần mềm được cài đặt mà bị hư hỏng đòi hỏi phải cài đặt lại (tuy nhiên, xem [System File Checker](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/System_File_Checker&usg=ALkJrhjTCsTReJiXe2c8__BYM-fpVyUC7Q) ).
* **Vấn đề Firmware**

***Firmware*** *là một thuật ngữ thỉnh thoảng được dùng để biểu thị những phần mềm cố định, thường là khá nhỏ, để điều khiển nội quan nhiều thiết bị điện tử*

* Hoạt động phần mềm chống virus có thể gây trở ngại với một [firmware](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Firmware&usg=ALkJrhj1zncYrfT61rceKWO4asD2WHFFoA) . Bất kỳ firmware khả năng ghi trong máy tính có thể bị nhiễm mã độc.Đây là một mối quan tâm lớn, như là một nhiễm [BIOS](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/BIOS&usg=ALkJrhhmtvacJoPmR_Tar3f8YWQ8E0SbCw) có thể yêu cầu các chip BIOS thực tế để có thay thế để đảm bảo mã độc được loại bỏ hoàn toàn. phần mềm chống virus là không có hiệu quả bảo vệ phần mềm và các [bo mạch chủ](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/Motherboard&usg=ALkJrhh5ZTQHqICBrt1K6Iia08d1Tp-Bqw) BIOS khỏi bị nhiễm trùng. Trong năm 2014, các nhà nghiên cứu bảo mật đã phát hiện ra rằng [USB](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/USB&usg=ALkJrhgm4ft4MGtBrqs1J7--pY3cjGH9hg) thiết bị chứa firmware cho phép ghi lại có thể được sửa đổi với mã độc hại (với tên gọi " [BadUSB](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com.vn&sl=en&u=https://en.wikipedia.org/wiki/BadUSB&usg=ALkJrhgK9yVflkylD090mg75VDg9UCQBXw) "), mà phần mềm chống virus không thể phát hiện hoặc ngăn chặn.Các mã độc có thể chạy không bị phát hiện trên máy tính và thậm chí có thể lây nhiễm sang các hệ điều hành trước khi nó khởi động lên.

1. **Firewall**

***Mặc dù Internet là mỏ thông tin và giao tiếp xã hội quý giá, nhưng không phải lúc nào nó cũng thân thiện. Thay vào đó, có rất nhiều kẻ xấu rình rập trên mạng với mưu đồ xâm nhập vào những máy tính kết nối với Internet.***

Hàng phòng vệ đầu tiên chống lại những kẻ hay đi xâm nhập trộm là firewall: một tập hợp những thủ thuật chuyên môn có thể giúp ngăn chặn ý đồ xâm nhập xấu vào máy tính và hạn chế những gì đi ra khỏi máy

1. Thế nào là firewall

Trong ngành [mạng máy tính](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_m%C3%A1y_t%C3%ADnh), firewall () là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong [mạng nội bộ](https://vi.wikipedia.org/wiki/LAN)

1. Nhiệm vụ firewall

Nhiệm vụ cơ bản của tường lửa là kiểm soát giao thông dữ liệu giữa hai vùng có độ tin cậy khác nhau. Các vùng tin cậy (*zone of trust*) điển hình bao gồm: mạng [Internet](https://vi.wikipedia.org/wiki/Internet) (vùng không đáng tin cậy) và [mạng nội bộ](https://vi.wikipedia.org/wiki/Intranet) (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên [nguyên tắc quyền tối thiểu](https://vi.wikipedia.org/w/index.php?title=Nguy%C3%AAn_t%E1%BA%AFc_quy%E1%BB%81n_t%E1%BB%91i_thi%E1%BB%83u&action=edit&redlink=1) (*principle of least privilege*)

1. Phân loại firewall

**Firewall cứng:** Chủ yếu được dùng trong mạng lớn có nhiều máy tính và đặt tại các trung tâm xứ lý luồng dữ liệu ra vào với bên ngoài như các đầu mối giao tiếp của hệ thống máy tính của quốc gia, tổ chức, của doanh nghiệp lớn, ngân hàng v.v... ra vào với môi trường bên ngoài. Chi phí để đầu tư cho các thiết bị này rất đắt tiền, không phù hợp với các doanh nghiệp có quy mô nhỏ. Cisco, SonicWALL, Barracuda và WatchGuard là những nhãn hiệu có thị phần lớn, có uy tín trên thị trường thiết bị bảo mật, tường lửa và được cấp chứng chỉ ICSA, một chứng chỉ chuẩn công nghiệp thế giới cho việc thanh tra, kiểm tra gói dữ liệu. Ngoài ra, một số thiết bị truy cập mạng cũng có chức năng tường lửa như modem ADSL, thiết bị phát sóng internet wifi v.v... nhưng đây là những tường lửa cơ bản, các hacker rất dễ vượt qua.

**Firewall mềm:** Được ứng dụng phổ biến hơn, đa dạng về chủng loại, trong đó có loại tích hợp trong các bộ phần mềm diệt virus, có loại dùng chuyên biệt cho máy chủ và có độ phức tạp trong cấu hình, đòi hỏi phải có nhân viên quản trị mạng am hiểu về nó, ví dụ như: ISA (Microsoft Internet Security and Acceleration Server), Proxy Server. Ngoài ra, trong hầu hết các hệ điều hành đều có tích hợp sẵn phần mềm tường lửa cơ bản và nó được thiết kế cao cấp hơn khi tích hợp trong các hệ điều hành dùng cho máy chủ.

Phân loại theo phạm vi của cá truyền thông được lọc

Có 2 loại tường lửa thông dụng là **tường lửa bảo vệ** để bảo vệ an ninh cho máy tính cá nhân hay mạng cục bộ, tránh sự xâm nhập, tấn công từ bên ngoài và **tường lửa ngăn chặn** thường do các [nhà cung cấp dịch vụ Internet](https://vi.wikipedia.org/wiki/Nh%C3%A0_cung_c%E1%BA%A5p_d%E1%BB%8Bch_v%E1%BB%A5_Internet) thiết lập và có nhiệm vụ ngăn chặn không cho máy tính truy cập một số trang web hay máy chủ nhất định, thường dùng với mục đích [kiểm duyệt Internet](https://vi.wikipedia.org/wiki/Ki%E1%BB%83m_duy%E1%BB%87t_Internet).

1. Nguyên lý hoạt động của firewall

Khi nói đến việc l­u thông dữ liệu giữa các mạng với nhau thông qua Firewall thì điều đó có nghĩa rằng Firewall hoạt động chặt chẽ với giao thức TCI/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận đ­ợc từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data pakets) rồi gán cho các paket này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các packet và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận đ­ợc. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng.Đó là:

* Địa chỉ IP nơi xuất phát ( IP Source address)
* Địa chỉ IP nơi nhận (IP Destination address)
* Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)
* Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)
* Cổng TCP/UDP nơi nhận (TCP/UDP destination port)
* Dạng thông báo ICMP ( ICMP message type)
* Giao diện packet đến ( incomming interface of packet)
* Giao diện packet đi ( outcomming interface of packet)

Nếu luật lệ lọc packet đ­ược thoả mãn thì packet đ­ợc chuyển qua firewall. Nếu không packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản đ­ợc các kết nối vào các máy chủ hoặc mạng nào đó đ­ợc xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) đ­ợc phép mới chạy được trên hệ thống mạng cục bộ.

1. Chức năng của firewall

FireWall bảo vệ chống lại những sự tấn công từ bên ngoài.

* Tấn công trực tiếp:

Cách thứ nhất là dùng phương pháp dò mật khẩu trực tiếp. Thông qua các chương trình dò tìm mật khẩu với một số thông tin về người sử dụng như ngày sinh, tuổi, địa chỉ v.v…và kết hợp với thư viện do người dùng tạo ra, kẻ tấn công có thể dò được mật khẩu của bạn. Trong một số trường hợp khả năng thành công có thể lên tới 30%.

Cách thứ hai là sử dụng lỗi của các chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được để chiếm quyền truy cập (có được quyền của người quản trị hệ thống).

* Nghe trộm:

Có thể biết được tên, mật khẩu, các thông tin chuyền qua mạng thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền qua mạng.

* Giả mạo địa chỉ IP.
* Vô hiệu hoá các chức năng của hệ thống (deny service).

Đây là kiểu tấn công nhằm làm tê liệt toàn bộ hệ thống không cho nó thực hiện các chức năng mà nó được thiết kế. Kiểu tấn công này không thể ngăn chặn được do những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

* Lỗi người quản trị hệ thống.
* Yếu tố con người với những tính cách chủ quan và không hiểu rõ tầm quan trọng của việc bảo mật hệ thống nên dễ dàng để lộ các thông tin quan trọng cho hacker.

1. Ưu, nhược điểm của firewall
2. *Ưu điểm*

* Firewall có thể bảo vệ hệ thống máy tính chống lại những kẻ đột nhập qua khả năng ngăn chặn những phiên làm việc từ xa (remote login).
* Ngăn chặn thông tin từ bên ngoài (Internet) vào trong mạng được bảo vệ, trong khi cho phép người sử dụng hợp pháp được truy nhập tự do mạng bên ngoài.
* Firewall ngăn chặn các dịch vụ ít tin cậy.
* Truy nhập có điều khiển đến từng host.
* Tập trung hóa chính sách bảo mật.
* Xác nhận người dùng và lưu trữ thông tin.

1. *Nhược điểm*

* Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.
* Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không “đi qua” nó. Một cách cụ thể, Firewall không thể chống lại một cuộc tấn công từ một đường dial–up, hoặc sự mất mát thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.
* Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data–drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua Firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.
* Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của
* **Khả năng tường lửa bị vượt qua:** Vấn đề con người giữ vai trò rất quan trọng trong thiết lập, cấu hình và quản trị tường lửa một cách thường xuyên liên tục. Ví dụ: một trang web có nội dung xấu nào đó bị tường lửa chặn lại thì người thiết kế trang web đó cũng có thể trỏ nó đến một tên miền khác nữa, với tên miền mới này thì tường lửa chưa biết và chưa cấm do đó nội dung trang web xấu đó vẫn lọt qua được. Một giải pháp khác nữa đó là hacker thiết kế riêng hẳn một trang web để dành vượt tường lửa. Trang web này có dạng giống trang web google, chỉ có một ô duy nhất cho phép gõ vào địa chỉ trang web nhưng bất cứ trang web nào bị tường lửa cấm thì khi gõ địa chỉ của nó trong ô này đều có thể truy cập được một cách dễ dàng. Để đánh cắp thông tin dữ liệu phổ biến nhất là hacker tấn công qua telnet, truy cập trái phép vào một máy tính nào đó khi biết địa chỉ IP của nó trên mạng Internet. Trong trường hợp công ty có “nội gián” cung cấp tên máy, IP ra bên ngoài thì hacker cũng rất dễ dàng vượt qua tường lửa để lấy cắp thông tin dữ liệu. Ngoài ra, cách dùng các đoạn mã nguy hiểm ẩn nấp trong các gói dữ liệu “quen thuộc” để vượt qua tường lửa lấy cắp thông tin cũng ngày càng gia tăng. Nếu sử dụng phần mềm tường lửa không cao cấp, chuyên nghiệp, quản trị viên cấu hình không chặt chẽ, cập nhật thường xuyên thì hacker vẫn có khả năng tấn công để vượt qua tường lửa mà lấy cắp thông tin dữ liệu của tổ chức, công ty, cá nhân.

**Kết luận**: Ngày nay, trình độ của các hacker ngày càng giỏi hơn, trong khi đó các hệ thống mạng vẫn còn chậm chạp trong việc xử lý các lỗ hổng của mình. Điều này đòi hỏi người quản trị mạng phải có kiến thức tốt về bảo mật mạng để có thể giữ vững an toàn cho thông tin của hệ thống. Đối với người dùng cá nhân, họ không thể biết hết các thủ thuật để tự xây dựng cho mình một Firewall, nhưng cũng nên hiểu rõ tầm quan trọng của bảo mật thông tin cho mỗi cá nhân, qua đó tự tìm hiểu để biết một số cách phòng tránh những sự tấn công đơn giản của các hacker.

# Phần Ba: Kết luận