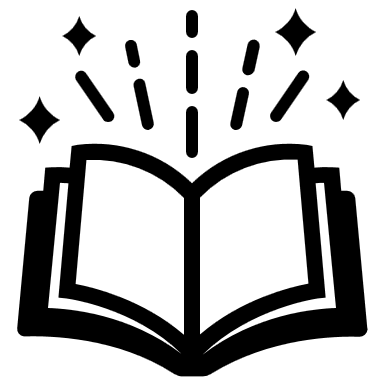
**ĐẠI HỌC HUẾ**

**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**KHOA CÔNG NGHỆ THÔNG TIN**

**MÔN AN NINH MẠNG**

****

**ĐỀ TÀI:**

**“TÌM HIỂU VỀ HỆ THỐNG TƯỜNG LỬA FIREWALL”**

**A blue and white sign with a white and red symbol

Description automatically generated**

**Giảng viên hướng dẫn: Võ Việt Dũng**

**Nhóm học phần: Nhóm 6**

**Nhóm thực hiện: Nhóm 9**

**Các thành viên:**

**- Châu Đăng Bảo Nguyên (Nhóm trưởng)**

**- Trương Đinh Minh Hiếu**

**- Nguyễn Tống Bảo Phúc**

**- Đỗ Thanh Nhật Nam**

**- Lê Văn Minh**

**- Đỗ Thái Bảo**

[**Mở đầu** 1](#_Toc187351052)

[**CHƯƠNG I: TỔNG QUAN VỀ FIREWALL** 2](#_Toc187351053)

[**1. Khái niệm** 2](#_Toc187351054)

[**2. Chức năng của Firewall** 2](#_Toc187351055)

[*2.1. Kiểm soát lưu lượng mạng* 2](#_Toc187351056)

[*2.2. Ngăn chặn tấn công mạng* 3](#_Toc187351057)

[*2.3. Quản lý và giám sát lưu lượng* 3](#_Toc187351058)

[*2.4. Quản lý truy cập* 4](#_Toc187351059)

[**3. Phân loại Firewall** 4](#_Toc187351060)

[*3.1. Dựa trên loại hệ thống được bảo vệ* 4](#_Toc187351061)

[*3.2. Dựa trên kiểu vật lý* 5](#_Toc187351062)

[*3.3. Dựa trên vị trí trong cấu trúc hạ tầng mạng* 5](#_Toc187351063)

[*3.4. Dựa trên phương thức lọc dữ liệu* 5](#_Toc187351064)

[**4. Ứng dụng của Firewall** 6](#_Toc187351065)

[**CHƯƠNG II: NHỮNG THIẾT KẾ CƠ BẢN CỦA FIREWALL** 7](#_Toc187351066)

[**1.Dual-homed Host** 7](#_Toc187351067)

[**2. Kiến trúc Screened Host** 9](#_Toc187351068)

[**3. Kiến trúc Screened Subnet Host** 10](#_Toc187351069)

[**4. Sử dụng nhiều Bastion Host** 11](#_Toc187351070)

[**5. Kiến trúc ghép chung Router trong và Router ngoài** 12](#_Toc187351071)

[**6. Kiến trúc ghép chung Bastion Host và Router ngoài** 13](#_Toc187351072)

[**CHƯƠNG III: CÁC THÀNH PHẦN VÀ CƠ CHẾ HOẠT ĐỘNG CỦA FIREWALL** 14](#_Toc187351073)

[**1. Bộ lọc gói tin (Packer Filtering):** 14](#_Toc187351074)

[1.1. Nguyên lí hoạt động 14](#_Toc187351075)

[*1.2. Ưu điểm và nhược điểm của Firewall sử dụng Packet Filter* 15](#_Toc187351076)

[**2. Cổng ứng dụng (Application-level Gateway)** 15](#_Toc187351077)

[*2.1. Nguyên lí hoạt động* 15](#_Toc187351078)

[*2.2. Ưu điểm và nhược điểm* 17](#_Toc187351079)

[**3. Cổng vòng (Circuit- level Gateway)** 17](#_Toc187351080)

[**4. Chính sách mạng (Network policy)** 18](#_Toc187351081)

[**5. Xác thực nâng cao (Advanced authentication)** 19](#_Toc187351082)

[**CHƯƠNG 4: GIẢI PHÁP FIREWALL CHO DOANH NGHIỆP** 21](#_Toc187351083)

[**1. Lợi ích khi triển khai hệ thống Firewall cho doanh nghiệp** 21](#_Toc187351084)

[**2. Một số giải pháp Firewall cho doanh nghiệp** 22](#_Toc187351085)

[**TÀI LIỆU THAM KHẢO** 27](#_Toc187351086)

# **Mở đầu**

Trong thời đại cách mạng công nghiệp 4.0, công nghệ thông tin đã trở thành trụ cột không thể thiếu trong mọi lĩnh vực của đời sống, từ kinh doanh, giáo dục, y tế cho đến quản lý nhà nước. Với sự kết nối toàn cầu mà mạng Internet mang lại, chúng ta đang chứng kiến một thế giới ngày càng phụ thuộc vào các hệ thống mạng để lưu trữ, xử lý, và trao đổi thông tin. Tuy nhiên, đi cùng với sự tiện lợi này là những thách thức to lớn về an ninh mạng. Từ những cuộc tấn công mạng có tổ chức, các phần mềm độc hại, cho đến các hành vi đánh cắp dữ liệu, thế giới số đang phải đối mặt với những rủi ro ngày càng phức tạp và nguy hiểm.

Đứng trước bối cảnh đó, Firewall (tường lửa) đã trở thành một trong những công cụ quan trọng nhất trong việc bảo vệ hệ thống mạng. Được ví như “người gác cổng” giữa mạng nội bộ và thế giới bên ngoài, Firewall không chỉ giúp kiểm soát luồng thông tin ra vào hệ thống mà còn hỗ trợ ngăn chặn các mối đe dọa từ những nguồn truy cập không đáng tin cậy. Qua thời gian, công nghệ Firewall cũng không ngừng được cải tiến để đối phó với các hình thức tấn công mạng ngày càng tinh vi, từ việc phát hiện các lỗ hổng bảo mật đến việc thiết lập các quy tắc phức tạp nhằm kiểm soát luồng dữ liệu.

Tuy nhiên, không phải ai cũng hiểu rõ về cách hoạt động của Firewall, vai trò của nó trong hệ thống an ninh mạng, cũng như những hạn chế mà công cụ này gặp phải. Điều này càng trở nên quan trọng khi các tổ chức và doanh nghiệp, đặc biệt là tại Việt Nam, đang phải đối mặt với sự gia tăng của các mối đe dọa mạng từ trong nước lẫn quốc tế.

Sau đây, bài tiểu luận của nhóm sẽ cung cấp những thông tin tổng quan về Firewall, những thiết kế cơ bản, các thành phần và cơ chế hoạt động của Firewall và một số giải pháp Firewall cho doanh nghiệp.

# **CHƯƠNG I: TỔNG QUAN VỀ FIREWALL**

## **1. Khái niệm**

Firewall (hay còn được gọi là “tường lửa”) được bắt nguồn từ bức tường được thiết kế trong các công trình để hạn chế hoả hoạn trong xây dựng. Đối với lĩnh vực công nghệ thông tin, Firewall được biết đến là một hệ thống bảo mật mạng giúp kiểm soát và giám sát lưu lượng dữ liệu giữa các mạng hoặc giữa thiết bị mạng và các nguồn bên ngoài (chẳng hạn như Internet). Mục tiêu của Firewall là bảo vệ hệ thống mạng khỏi các truy cập trái phép, tấn công mạng và các mối đe dọa khác, đồng thời cho phép các giao tiếp hợp lệ.

A diagram of a firewall

Description automatically generated

Firewall hoạt động bằng cách áp dụng các quy tắc lọc (filtering rules) cho các gói dữ liệu (packets) đi qua hệ thống của nó. Những quy tắc này có thể dựa trên nhiều yếu tố như địa chỉ IP nguồn, địa chỉ IP đích, cổng mạng (port), giao thức mạng (protocol) và nội dung trong các gói tin. Firewall có thể được triển khai dưới dạng phần mềm hoặc phần cứng, và có thể bảo vệ nhiều hệ thống, từ các máy tính cá nhân đến các mạng của các tổ chức, doanh nghiệp lớn.

## **2. Chức năng của Firewall**

Firewall thực hiện nhiều chức năng quan trọng để bảo vệ mạng và hệ thống khỏi các mối đe dọa. Các chức năng này có thể được chia thành các nhóm chính sau:

### *2.1. Kiểm soát lưu lượng mạng*

* Lọc gói tin (Packet Filtering):

Lọc gói tin là một trong những chức năng cơ bản của Firewall. Firewall kiểm tra mỗi gói dữ liệu mà nó nhận được và kiểm tra các thông số như địa chỉ IP nguồn, địa chỉ IP đích, số cổng, và giao thức (TCP, UDP, ICMP,...). Nếu các thông số này khớp với các quy tắc trong Firewall, gói tin sẽ được phép đi qua; nếu không, gói tin sẽ bị từ chối.

* Kiểm tra trạng thái (Stateful Inspection):

Đây là một phương pháp bảo mật cao hơn so với lọc gói tin thông thường. Khi Firewall thực hiện kiểm tra trạng thái, nó không chỉ kiểm tra các gói tin đơn lẻ mà còn theo dõi toàn bộ kết nối mạng. Mỗi kết nối sẽ có một trạng thái được ghi nhận (ví dụ, kết nối đã được thiết lập, kết nối đang mở, hay kết nối đã đóng). Firewall sẽ so sánh các gói tin đến với trạng thái của các kết nối hiện có và chỉ cho phép các gói tin hợp lệ của các kết nối hợp lệ.

### *2.2. Ngăn chặn tấn công mạng*

* Phát hiện ngăn chặn và xâm nhập (IDS/IPS):

Các Firewall hiện đại có thể tích hợp hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS). Hệ thống IDS phát hiện các hành vi bất thường trong lưu lượng mạng và có thể cảnh báo quản trị viên. Trong khi đó, hệ thống IPS không chỉ phát hiện mà còn ngăn chặn các cuộc tấn công ngay lập tức bằng cách ngừng các kết nối đáng ngờ.

* Chống phần mềm độc hại:

Firewall có thể kiểm tra dữ liệu vào và ra từ các hệ thống để phát hiện phần mềm độc hại (malware). Một số Firewall hiện đại có khả năng lọc các tệp đính kèm email hoặc tải xuống từ các trang web có nguy cơ chứa virus, trojan, spyware và các phần mềm độc hại khác. Điển hình như việc ta luôn nhận được các cảnh báo khi tải các tệp độc hại từ các trang web không đáng tin cậy.

### *2.3. Quản lý và giám sát lưu lượng*

* Giám sát lưu lượng mạng:

Firewall liên tục theo dõi lưu lượng mạng đi qua nó. Các hoạt động này có thể được ghi lại trong các nhật ký (logs) và cung cấp thông tin chi tiết về các kết nối mạng, người dùng, và ứng dụng. Firewall có thể ghi lại các địa chỉ IP đang cố gắng truy cập vào các cổng bị cấm và gửi cảnh báo nếu có dấu hiệu bất thường.

* Cảnh báo và báo cáo bảo mật:

Nhiều Firewall hiện đại có thể tạo ra các báo cáo chi tiết về các sự kiện bảo mật trong mạng. Các báo cáo này có thể bao gồm các thông tin như các cuộc tấn công đã bị chặn, số lượng kết nối đáng ngờ, và các lỗ hổng bảo mật trong hệ thống. Điều này giúp các quản trị viên theo dõi tình trạng bảo mật của hệ thống và đưa ra các biện pháp cải thiện.

### *2.4. Quản lý truy cập*

* Quy định quyền truy cập:

Firewall có thể được cấu hình để chỉ cho phép một số địa chỉ IP hoặc người dùng nhất định truy cập vào hệ thống. Quyền truy cập này có thể áp dụng cho cả người dùng trong nội bộ và người dùng từ bên ngoài. Chẳng hạn như ta chỉ cho phép nhân viên trong công ty truy cập vào các máy chủ quan trọng, trong khi chặn các kết nối từ các địa chỉ IP không đáng tin cậy.

## **3. Phân loại Firewall**

A diagram of a network

Description automatically generated

Firewall thường được phân loại dựa trên loại hệ thống mà nó bảo vệ, kiểu vật lý, vị trí được đặt trong cấu trúc hạ tầng mạng hoặc phương thức lọc dữ liệu.

### *3.1. Dựa trên loại hệ thống được bảo vệ*

* Network Firewall: Bảo vệ toàn bộ hệ thống mạng bằng cách giám sát và kiểm soát lưu lượng vào ra dựa trên các giao thức bảo mật được thiết lập sẵn.
* Host-based Firewall: Được cài đặt trên từng thiết bị hoặc máy chủ cụ thể, loại Firewall này bảo vệ và giám sát lưu lượng vào ra từ thiết bị đó.

### *3.2. Dựa trên kiểu vật lý*

* Hardware Firewall: Là một thiết bị Firewall vật lý độc lập, được lắp đặt giữa các thành phần mạng và các thiết bị kết nối. Các Firewall phần cứng này có thể xử lý được lưu lượng mạng lớn và cung cấp bảo mật mạnh mẽ cho hệ thống.
* Software Firewall: Là Firewall hoạt động dưới dạng phần mềm, có thể được triển khai trên các máy chủ hoặc máy tính cá nhân để bảo vệ hệ thống khỏi các mối đe doạ
* Cloud Firewall: Được triển khai trên đám mây (cloud), giúp bảo vệ các tài nguyên trên không gian đám mây và có khả năng mở rộng linh hoạt.

### *3.3. Dựa trên vị trí trong cấu trúc hạ tầng mạng*

* Internal Firewall: hay còn gọi là Firewall nội bộ, được đặt bên trong mạng thay vì ở rìa, nhằm bảo vệ các mối đe doạ trong nội bộ hệ thống.
* Distributed Firewall: Firewall phân tán là một giải pháp mở rộng, trong đó hệ thống Firewall được phân bố trên nhiều thiết bị khác nhau hoặc máy chủ
* Perimiter Firewall: được đặt tại rìa hoặc ranh giới giữa các hệ thống mạng, Firewall vành đai có tác dụng kiểm soát lưu lượng ra và vào mạng.

### *3.4. Dựa trên phương thức lọc dữ liệu*

* Next Generation Firewall – NGFW: Firewall thế hệ mới là một công nghệ tiên tiến kết hợp các chức năng truyền thống với các chức năng nâng cao như IPS và kiểm tra lưu lượng mã hoá.
* Packet Filtering Firewall: Firewall lọc gói tin kiểm tra từng gói dữ liệu được gửi đến hệ thống mạng. Nếu gói dữ liệu phù hợp với giao thức bảo mật đã được thiết lập sẵn sẽ được phép đi qua hoặc sẽ bị từ chối nếu không phù hợp.
* Circuit Level Gateway: hoạt động ở tầng phiên (session layer), loại Firewall này đảm bảo tính hợp lệ của các gói tin trong một kết nối thử. Sau khi được xác nhận, một kết nối liên tục giữa các mạng sẽ được cho phép.
* Web Application Firewall: được thiết kế để bảo vệ các ứng dụng web, giải pháp này sẽ lọc, giám sát và ngăn chặn lưu lượng HTTP đi đến ứng dụng web, bảo vệ các mối đe doạ tấn công như cross-site scripting (XSS) và SQL injection.
* Proxy Firewall : hoạt động ở tầng ứng dụng (application layer), loại Firewall này đóng vai trò trung gian cho các yêu cầu từ clients. Các yêu cầu sẽ được cho phép hoặc chặn giữa trên các quy tắc đã thiết lập sẵn.
* Stateful Inspection Firewall : là loại Firewall ghi nhớ các kết nối đang hoạt động trước đó, các quyết định được đưa ra dựa trên bộ quy tắc được cài đặt sẵn và ngữ cảnh, đồng thời nó còn theo dõi trạng thái của các kết nối đang hoạt động.

## **4. Ứng dụng của Firewall**

Nếu máy tính của bạn không được bảo vệ, khi kết nối với Internet, tất cả các luồng dữ liệu ra vào mạng đều được cho phép. Điều này có thể khiến cho thiết bị của bạn có thể bị tấn công bởi các hacker hay dính các đoạn mã độc, virus, trojan, … dẫn đến việc các thông tin cá nhân hoặc thông tin nhạy cảm khác của doanh nghiệp hay khách hàng có thể bị đánh cắp hoặc phá hoại. Tồi tệ hơn, các hacker xấu có thể mạo danh bạn và thực hiện các hoạt động phạm pháp. Do đó, việc cài đặt Firewall với vai trò là bức tường đầu tiên phát hiện và ngăn chặn các gói tin nhiễm độc trước khi chúng xâm nhập vào hệ thống của bạn.

Một số ứng dụng phổ biến của Firewall:

* Giám sát và lọc luồng giao thông mạng
* Ngăn chặn sự xâm nhập của virus
* Ngăn chặn các truy cập trái phép
* Bảo vệ dữ liệu và tài nguyên hệ thống

# **CHƯƠNG II: NHỮNG THIẾT KẾ CƠ BẢN CỦA FIREWALL**

## **1.Dual-homed Host**

Firewall kiến trúc kiểu Dual-homed host được xây dựng dựa trên máy tính dualhomed host. Một máy tính được gọi là dual-homed host nếu nó có ít nhất hai network interface, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau, do đó máy tính này đóng vai trò là router mềm. Kiến trúc dual - homed host rất đơn giản, máy dual - homed host ở giữa, một bên được nối với internet và bên còn lại nới với mạng nội bộ (mạng cần được bảo vệ). Gồm có các đặc điểm sau:

* Phải disable chức năng routing của dual-homed host để cấm hòan toàn lưu thông IP từ ngoài vào.
* Các hệ thống bên trong và bên ngoài dual-homed host chỉ có thể liên lạc với dual-homed host mà chúng không liên lạc trực tiếp được với nhau.
* Dual-homed host cung cấp dịch vụ thông qua proxy server hoặc login trực tiếp vào dual-homed host.

\*Ưu điểm của Dual-homed Host:

Cài đặt dễ dàng, không yêu cầu phần cứng hoặc phần mềm đặc biệt.

Dual-homed Host chỉ yêu cầu cấm khả năng chuyển các gói tin, do vậy, thông thường trên các hệ Unix, chỉ cần cấu hình và dịch lại nhân (Kernel) của hệ điều hành là đủ.

\*Nhược điểm của Dual-homed Host:

Không đáp ứng được những yêu cầu bảo mật ngày càng phức tạp, cũng như những hệ phần mềm mới được tung ra thị trường.

Không có khả năng chống đỡ những đợt tấn công nhằm vào chính bản thân nó, và khi Dual-homed Host đó bị đột nhập, nó sẽ trở thành đầu cầu lý tưởng để tấn công vào mạng nội bộ

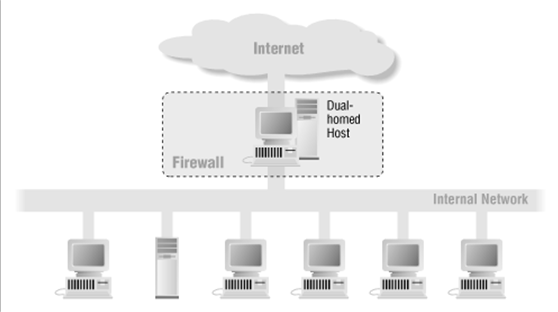
\* Đánh giá về Dual-homed Host:

Để cung cấp dịch vụ cho những người sử dụng mạng nội bộ có một số giải pháp như sau:

* Kết hợp với các Proxy Server cung cấp những Proxy Service.
* Cấp các tài khoản người dùng trên máy dual-homed host này và khi mà người sử dụng muốn sử dụng dịch vụ từ Internet hay dịch vụ từ external network thì họ phải logging in vào máy này.
* Phương pháp cấp tài khoản người dùng trên máy dual-homed host khá phức tạp, vì mỗi lần người dùng muốn sử dụng dịch vụ thì phải logging in vào máy khác (dual-homed host) khác với máy của họ, đây là vấn đề rất không thuận tiện với người sử dụng.
* Nếu dùng Proxy Server: khó có thể cung cấp được nhiều dịch vụ cho người sử dụng vì phần mềm Proxy Server và Proxy Client không phải loại dịch vụ nào cũng có sẵn. Hoặc khi số dịch vụ cung cấp nhiều thì khả năng đáp ứng của hệ thống có thể giảm xuống vì tất cả các Proxy Server đều đặt trên cùng một máy.

Một khuyết điểm cơ bản của hai mô hình trên nữa là : khi mà máy dualhomed host nói chung cũng như các Proxy Server bị đột nhập vào. Người tấn công (attacker) đột nhập được vào hệ thống sẽ hiểu các dịch vụ trên hệ thống đó, nắm bắt được các điểm yếu và thực hiện các hành vi phá hoại tinh vi hơn.

Trong các hệ thống mạng dùng Ethernet hoặc Token Ring thì dữ liệu lưu thông trong hệ thống có thể bị bất kỳ máy nào nối vào mạng đánh cắp dữ liệu cho nên kiến trúc này chỉ thích hợp với một số mạng nhỏ.



## **2. Kiến trúc Screened Host**

Trong kiến trúc này chức năng bảo mật chính được cung cấp bởi chức năng packet filtering tại screening router.

Packet filtering trên screening router được setup sao cho bastion host là máy duy nhất trong internal network mà các host trên internet có thể mở kết nối đến. Packet filtering cũng cho phép bastion host mở các kết nối(hợp pháp) ra bên ngoài(external network).

Thường Packet filtering thực hiện các công việc như sau :

* Cho phép các internal hosts mở kết nối đến các host trên internet đối với một số dịch vụ được phép.
* Cấm tất cả kết nối từ các internal hosts .

Khi hacker đã tấn công được vào bastion host thì không còn một rào chắn nào cho các internal hosts.

\*Ưu điểm:

* Ba tầng bảo vệ: Router ngoài, Máy chủ, và Router trong.
* Chỉ có một số hệ thống đã được chọn ra trên mạng trung gian là được biết đến bởi Internet qua bảng thông tin định tuyến và trao đổi thông tin định tuyến DNS (Domain Name Server).
* Đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ Proxy.

\*Đánh giá về kiến trúc Screend Subnet Host

Đối với những hệ thống yêu cầu cung cấp dịch vụ nhanh, an toàn cho nhiều người sử dụng đồng thời cũng như khả năng theo dõi lưu thông của mỗi người sử dụng trong hệ thống và dữ liệu trao đổi giữa các người dùng trong hệ thống cần được bảo vệ thì kiến trúc cơ bản trên phù hợp.

Để tăng độ an toàn trong mạng nội bộ, kiến trúc screened subnet ở trên sử dụng thêm một mạng DMZ (DMZ hay perimeter network) để che phần nào lưu thông bên trong mạng nội bộ. Tách biệt mạng nội bộ với Internet.

Sử dụng 2 Screening Router (bộ định tuyến lọc): Router ngoài và Router trong.

Áp dụng qui tắc dư thừa có thể bổ sung thêm nhiều mạng trung gian (DMZ và perimeter network) càng tăng khả năng bảo vệ càng cao.

Ngoài ra, còn có những kiến trúc biến thể khác như: sử dụng nhiều Bastion Host (máy chủ) (Máy chủ), ghép chung Router trong và Router ngoài, ghép chung Bastion Host (máy chủ) (Máy chủ) và Router ngoài.

Diagram of a computer network

Description automatically generated

## **3. Kiến trúc Screened Subnet Host**

Thêm môt perimeter network để cô lập internal network với internet. Như vậy dù hacker đã tấn công được vào bastion host vẫn còn một rào chắn nữa phải vượt qua là interior router. Các lưu thông trong internal network được bảo vệ an toàn cho dù bastion đã bị“chiếm”. Các dịch vụ nào ít tin cậy và có khảnăng dễ bị tấn công thì nên để ở perimeter network. Bastion host là điểm liên lạc cho các kết nối từ ngoài vào như: SMTP; FTP, DNS. Còn đối với việc truy cập các dịch vụ từ internal clients đến các server trên internet thì được điều khiển như sau :

* Set up packet filtering trên cả hai exterior và interior router để cho phép internal clients truy cập các servers bên ngoài một cách trực tiếp.
* Set up proxy server trên bastion host để cho phép internal clients truy cập các servers bên ngoài một cách gián tiếp.

A diagram of a network

Description automatically generated

## **4. Sử dụng nhiều Bastion Host**

Với mô hình này thì tốc độ đáp ứng cho những người sử dụng bên trong (local user) một phần nào đó không bị ảnh hưởng bởi những hoạt động của người sử dụng bên ngoài mạng (external user).

\*Sử dụng nhiều Bastion Host mang lại nhiều lợi ích, bao gồm:

* **Phân tách chức năng:** Mỗi Bastion Host có thể được chuyên môn hóa để xử lý một loại dịch vụ hoặc ứng dụng cụ thể, chẳng hạn:
  + Bastion Host 1: Xử lý máy chủ web.
  + Bastion Host 2: Xử lý máy chủ email.
  + Bastion Host 3: Máy chủ DNS hoặc ứng dụng khác.
* **Tăng cường bảo mật:**
  + Nếu một Bastion Host bị tấn công, những Bastion Host khác sẽ không bị ảnh hưởng.
  + Phân tách giúp giảm thiểu phạm vi tấn công (Attack Surface) và **đảm bảo tính sẵn sàng cao (High Availability)**
  + Nếu một Bastion Host gặp sự cố hoặc bị xâm nhập, các Bastion Host khác vẫn hoạt động bình thường, đảm bảo dịch vụ không bị gián đoạn.
* **Cân bằng tải và hiệu suất:** Sử dụng nhiều Bastion Host giúp chia sẻ tải giữa các hệ thống, tránh tình trạng quá tải.
* **Kiểm soát truy cập tốt hơn:** Cung cấp khả năng định nghĩa các chính sách truy cập chi tiết hơn dựa trên vai trò của từng Bastion Host.

\***Ưu điểm của kiến trúc nhiều Bastion Host**

* **Độ tin cậy cao:** Giảm nguy cơ một Bastion Host bị xâm nhập làm gián đoạn toàn bộ hệ thống.
* **Khả năng mở rộng:** Dễ dàng thêm Bastion Host mới khi cần hỗ trợ thêm dịch vụ hoặc tăng tải.
* **Cách ly dịch vụ:** Phân chia rõ ràng trách nhiệm của từng Bastion Host, giúp bảo trì và quản lý dễ dàng hơn.
* **Giảm tải cho từng máy chủ:** Tối ưu hóa hiệu suất vì mỗi Bastion Host chỉ xử lý một phần nhiệm vụ.

\***Nhược điểm và thách thức**

* **Chi phí triển khai cao:** Cần nhiều tài nguyên phần cứng, phần mềm và nhân sự.
* **Phức tạp trong quản lý:** Phải giám sát, cập nhật và bảo trì nhiều Bastion Host cùng lúc.
* **Rủi ro phân quyền không đồng nhất:** Nếu chính sách bảo mật không đồng nhất giữa các Bastion Host, có thể tạo ra lỗ hổng bảo mật.

A computer screen shot of a computer

Description automatically generated

## **5. Kiến trúc ghép chung Router trong và Router ngoài**

Router phải cho phép áp dụng các luật cho dòng packet đi vô và đi ra trên mỗi interface.

Do ghép chung router trong và router ngoài nên kiến trúc này làm giảm đi lớp bảo vệ mạng bên trong, có thể nói kiến trúc ghép chung router trong và router ngoài nằm ở giữa kiến trúc Screened host và Screened Subnet host.

A diagram of a computer network

Description automatically generated

## **6. Kiến trúc ghép chung Bastion Host và Router ngoài**

Kiến trúc này chỉ sử dụng cho mạng chỉ có một đường nối dùng giao thức SLIP hoặc PPP ra internet.

Kiểu ghép chung Bastion host và router ngoài (Exterior router) này gần giống với Screened Subnet Host. Nó cho tốc độ đáp ứng thường thấp nhưng mà vẫn có thể chấp nhận được do tốt độ đường truyền thấp, chức năng lọc của router ngoài ít, chức năng lọc gói chủ yếu là router trong.

**A diagram of a computer network

Description automatically generated**

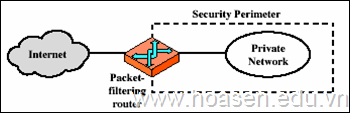
# **CHƯƠNG III: CÁC THÀNH PHẦN VÀ CƠ CHẾ HOẠT ĐỘNG CỦA FIREWALL**

## **1. Bộ lọc gói tin (Packer Filtering):**

### 1.1. Nguyên lí hoạt động

Khi nói đến việc lưu 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 TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được 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 packets) rồi gán cho các packet 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 gói tin cho phép hay từ chối packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong các số các rules hay không. Các rules này dựa trên các thông tin ở packet header bao gồm các thông tin sau:

* 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 gói tin (packet) đến (Incomming interface of packet).
* Giao diện gói tin (packet) đi (Outcomming interface of packet).

*Packet filtering router*

Nếu luật lệ lọc gói được thỏa mãn thì packet được chuyển qua Firewall, nếu không packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, 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 những dịch vụ nào đó (SSH, SMTP, FTP…) được phép mới chạy được trên hệ thống mạng cục bộ.

### *1.2. Ưu điểm và nhược điểm của Firewall sử dụng Packet Filter*

\*Ưu điểm:

* Đa số các hệ thống Firewall đều được sử dụng bộ lọc gói tin. Một trong những ưu điểm của phương pháp dùng bộ lọc gói là chi phí thấp vì cơ chế lọc gói đã có sẵn trong các router.
* Ngoài ra, bộ lọc gói là trong suốt đối với người sử dụng và các ứng dụng vì vậy nó không yêu cầu người sử dụng phải thao tác gì cả.

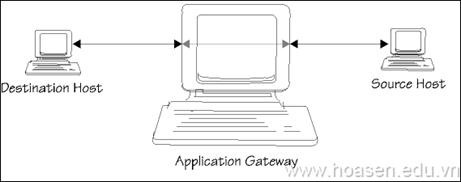
\*Nhược điểm:

* Việc định nghĩa các chế độ lọc gói là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ internet, các dạng packet header. Khi yêu cầu về lọc gói tin càng lớn, các rules càng trở nên phức tạp do đó rất khó quản lý và điều khiển.
* Do làm việc dựa trên header của các packet nên bộ lọc không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

## **2. Cổng ứng dụng (Application-level Gateway)**

### *2.1. Nguyên lí hoạt động*

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là proxy service. Proxy service là các bộ code đặc biệt cài đặt trên cổng ra (gateway) cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua Firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị cho là chấp nhận được trong khi từ chối những đặc điểm khác.



*Application Gateway*

Một cổng ứng dụng thường được coi như là một pháo đài (Bastion host) bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một Bastion host là:

* Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ điều hành (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào hệ điều hành (Operating system) cũng như là đảm bảo sự tích hợp Firewall.
* Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên Bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.
* Bastion host có thể yêu cầu nhiều mức độ khác nhau ví dụ như username và password hay smart card.

Mỗi proxy được cài đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của dữ liệu mạng đi qua nó. Điều này có nghĩ là bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy đều độc lập với các proxy khác trên bastion host. Điều này cho phép dễ dàng cài đặt một proxy mới hay tháo gỡ một proxy.

### *2.2. Ưu điểm và nhược điểm*

\* Ưu điểm:

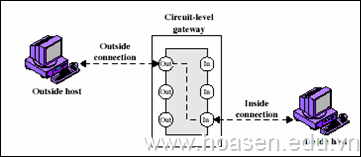
* Cho phép người quản trị hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy cập bởi các dịch vụ.
* Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là dịch vụ ấy bị khóa.
* Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt và nó có nhậy ký ghi chép lại thông tin về truy cập hệ thống.
* Luật lệ (Rule) lọc filtering cho cổng ứng dụng dễ dàng cấu hình và kiểm tra hơn so với bộ lọc gói.

\* Nhược điểm: Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet.

## **3. Cổng vòng (Circuit- level Gateway)**

Circuit Level Gateway – cổng vòng – là một chức năng đặc biệt có thể thực hiện bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ là chuyển tiếp các kết nối TCP mà không thực hiện bất kì một hành động xử lý hay lọc gói nào.

Hình sau minh họa một hành động sử dụng kết nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua Firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên vì sự kết nối này xuất hiện từ hệ thống Firewall nên nó che dấu thông tin về mạng nội bộ.



Circuit-level Gateway

Cổng vòng thường được sử dụng cho những kết nối ra ngoài. Ưu điểm lớn nhất là một Bastion host có thể được cấu hình như là một hỗn hợp cung cấp cổng ứng dụng cho những kết nối đến và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống Firewall dễ dàng sử dụng cho người dùng trong mạng nội bộ muốn trực tiếp truy câp tới các dịch vụ internet, trong khi vẫn cung cấp chức năng bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

## **4. Chính sách mạng (Network policy)**

Việc thiết kế, cài đặt và sử dụng Firewall trong mạng phần lớn chịu ảnh hưởng của hai cấp chính sách mạng — chính sách cấp cao hơn và chính sách cấp thấp hơn.

1. Chính sách cấp cao hơn là chính sách truy cập mạng cụ thể theo từng vấn đề, xác định các dịch vụ được phép hoặc bị từ chối rõ ràng từ mạng bị hạn chế, cách sử dụng chúng và các điều kiện ngoại lệ đối với chính sách này.
2. Chính sách cấp thấp hơn chỉ rõ cách Firewall sẽ xử lý hạn chế truy cập và lọc dịch vụ được định nghĩa trong chính sách cấp cao.

Các chính sách này được giải thích ngắn gọn dưới đây.

* Chính sách truy cập dịch vụ:
* Tập trung vào các vấn đề sử dụng cụ thể của internet và tất cả các truy cập mạng bên ngoài (ví dụ: chính sách quay số, kết nối SLIP và PPP).
* Để Firewall hoạt động hiệu quả, chính sách truy cập dịch vụ phải thực tế và hợp lý, đồng thời nên được soạn thảo trước khi triển khai Firewall.
* Một chính sách thực tế là một chính sách mang lại sự cân bằng giữa bảo vệ mạng khỏi các rủi ro đã biết trong khi vẫn cung cấp cho user quyền truy cập vào các tài nguyên mạng.
* Firewall có thể triển khai nhiều chính sách truy cập dịch vụ khác nhau. Tuy nhiên, một chính sách điển hình có thể là không cho phép truy cập từ Internet vào một trang web nhưng cho phép truy cập từ trang web ra Internet. Một chính sách điển hình khác có thể là cho phép truy cập từ Internet, nhưng chỉ đến các hệ thống được chọn như máy chủ thông tin và máy chủ email.
* Firewall thường triển khai các chính sách truy cập dịch vụ cho phép một số người dùng truy cập từ Internet đến các máy chủ nội bộ được chọn. Tuy nhiên, quyền truy cập này chỉ được cấp nếu cần thiết và chỉ khi nó có thể kết hợp với xác thực nâng cao.
* Chính sách thiết kế Firewall:
* Là chính sách cụ thể đối với Firewall và xác định các quy tắc được sử dụng để thực hiện chính sách truy cập dịch vụ. Không thể thiết kế chính sách này trong một môi trường tách biệt mà không hiểu rõ khả năng và hạn chế của Firewall cũng như các mối đe dọa và lỗ hổng liên quan đến TCP/IP.
* Firewall thường triển khai một trong hai chính sách thiết kế cơ bản**: cho phép mọi dịch vụ trừ khi bị từ chối rõ ràng và từ chối mọi dịch vụ trừ khi được phép rõ ràng.**
* Firewall thực hiện chính sách đầu tiên cho phép tất cả các dịch vụ truyền vào trang web theo mặc định, ngoại trừ các dịch vụ mà chính sách truy cập dịch vụ đã xác định là không được phép.Chính sách thứ hai tuân theo mô hình truy cập cổ điển được sử dụng trong tất cả các lĩnh vực bảo mật thông tin, trong đó chính sách thứ hai từ chối tất cả các dịch vụ theo mặc định nhưng sau đó chuyển tiếp các dịch vụ đã được xác định là được phép.

## **5. Xác thực nâng cao (Advanced authentication)**

Các biện pháp xác thực nâng cao như thẻ thông minh (smartcards), mã thông báo xác thực (authentication tokens), sinh trắc học (biometrics), và các cơ chế dựa trên phần mềm được thiết kế để khắc phục các điểm yếu của mật khẩu truyền thống. Mặc dù các kỹ thuật xác thực khác nhau, chúng có điểm chung là mật khẩu được tạo ra bởi các thiết bị xác thực nâng cao không thể bị kẻ tấn công sử dụng lại nếu đã theo dõi kết nối. Trước những vấn đề do mật khẩu gây ra trên internet, một Firewall có thể truy cập internet nhưng không sử dụng hoặc không hỗ trợ sử dụng xác thực nâng cao có thể được coi là không còn phù hợp trong bối cảnh hiện tại.

Một số thiết bị xác thực nâng cao phổ biến hiện nay được gọi là **hệ thống mật khẩu dùng một lần (one-time password systems)**. Vì mã thông báo hoặc thẻ hoạt động cùng với phần mềm hoặc phần cứng trên máy chủ, phản hồi được tạo ra sẽ là duy nhất cho mỗi lần đăng nhập. Kết quả là một mật khẩu dùng một lần, nếu bị theo dõi, cũng không thể được kẻ xâm nhập sử dụng lại để truy cập tài khoản.

# **CHƯƠNG 4: GIẢI PHÁP FIREWALL CHO DOANH NGHIỆP**

## **1. Lợi ích khi triển khai hệ thống Firewall cho doanh nghiệp**

Một số lợi ích khi triển khai hệ thống Firewall cho doanh nghiệp:

* Hạn chế hoặc ngăn chặn việc truy cập trái phép từ bên ngoài: Firewall được ví như một anh bảo vệ gách cộng tại công ty. Nhiệm vụ của giải pháp Firewall cho doanh nghiệp là sẽ ngăn chạn những người lạ vào công ty. Nếu ai đó muốn vào công ty, Firewall sẽ phải xác định đối tượng đó là ai? vào gặp ai? vào để làm gì? kiểm tra các thông tin của người vào như địa chỉ, ID của người vào. Nếu phát hiện là người lạ không được phép vào thì Firewall sẽ xóa bỏ kết nối truy cập đó và gửi báo cáo vào danh mục báo cáo.
* **Ngăn chặn các mã độc phát tán vào hệ thống mạng nội bộ**: Không chỉ là ngăn chặn các mã độc, các truy cập người lạ từ bên ngoài, Firewall cho doanh nghiệp còn có tác dụng ngăn chặn những đoạn mã độc phát tán trong máy tính nội bộ. Không ai đảm bảo rằng máy tính làm việc của nhân viên khi mang ra ngoài internet không nhiễm mã độc. Nếu máy tính làm việc nhân viên bị nhiễm, virus hoàn toàn có thể lây lan sáng máy tính khách trong công ty, rồi virus tìm cách xâm nhập vào máy chủ, chèn mã độc vào máy chủ. Giải pháp Firewall cho doanh nghiệp sẽ ngăn chặn những rui ro mã độc từ các máy tính nội bộ tấn công vào server.
* **Ngăn ngừa khả năng nhiễm virus từ các dữ liệu như Email, truy cập website internet:** Hiện nay hầu hết máy tính đều sử dụng Email và internet để làm việc. Khi sử dụng email và internet thì đây là 2 nguồn lây nhiễm mã độc tấn công mạng nhiều nhất. Khi người dùng truy cập các website trên internet có chứa virus, mã độc. Firewall sẽ phát hiện các đoạn mã độc hay các tập tin chứa virus và sẽ không cho người dùng tải chúng về máy tính hoặc là ngắt kết nối tới các trang website đó. Cũng tương tự Email. Nếu phát hiện Email có chứa mã độc hay tập tin đính kèm có virus. Giải pháp Firewall cho doanh nghiệp sẽ loại bỏ file đính kèm đó hoặc là ngăn chặn email đó không cho đi vào hệ thống máy chủ, máy tính của công ty.
* **Theo dõi và giám sát việc truy cập dữ liệu internet của nhân viên trong công ty:** Firewall cho doanh nghiệp không chỉ kiểm soát việc truy cập từ bên ngoài vào mà giải pháp Firewall còn giúp doanh nghiệp kiểm soát và quản lý nhân viên của công ty khi truy cập internet. Như ngăn chặn những website nhạy cảm, chơi game, thoi dõi việc sử dụng internet của nhân viên. Tháng này nhân viên A truy cập tới nhũng website nào nhiều nhất? Họ tải bao nhiêu dữ liệu về máy tính? Họ truy cập những nguồn website nào trên internet?
* **Kết nội mạng VPN an toàn, kết nối dữ liệu server mọi lúc mọi nơi:** Một tính năng cực kỳ quan trọng đối với Firewall cho doanh nghiệp đó chính là tính năng VPN . VPN hay còn gọi là mạng riêng ảo, tức là hệ thống sẽ tạo ra một kết nói riêng ảo trên đường truyền internet. Ở đó gói tin được truyền tải trên đường internet được mã hóa và ấn các địa chỉ IP kết nối public. Tính năng này doanh nghiêp thường sử dung khi nhân viên muốn làm việc ở nhà hoặc là khi nhân viên đi ra khỏi văn phòng làm việc của công ty nhưng phải kết nối các phần mềm về máy chủ của công ty để sử dụng dữ liêu. VPN tạo ra một kết nối an toàn giữa máy tính và máy chủ dữ liệu công ty. Mô hình VPN site to site cũng sẽ áp dụng cho doanh nghiệp có nhiều chi nhánh, có nhiều văn phòng. Việc truyền tải và liên kết dữ liệu giữa các chi nhánh, văn phòng
* **Hạn chế hoặc ngăn chặn một số phần mềm trên máy tính:** Firewall cho doanh nghiệp còn giúp doanh nghiệp hạn chế một số phần mềm hiện nay như Zalo, Skype, MS Team… tùy vào chính sách quản lý và chính sách bảo mật của mỗi khách hàng. Chúng tôi sẽ triển khai Firewall ngăn chặn hay cho phép những phần mềm phù hợp với yêu cầu của công ty.

## **2. Một số giải pháp Firewall cho doanh nghiệp**

* **Palo Alto:**

Palo Alto là nhà cung cấp bảo mật mạng hàng đầu trên thế giới, chuyên cung cấp các mẫu giải pháp Firewall tiên tiến cùng nhiều dịch vụ bảo mật chất lượng cao dành cho mọi môi trường doanh nghiệp.

Palo Alto cung cấp Firewall thế hệ mới dựa trên đám mây, máy ảo và vật lý. Dòng sản phẩm Palo Alto PA được thiết kế cho các trung tâm dữ liệu, nhà cung cấp dịch vụ, chi nhánh và điểm bán lẻ cũng như các khu công nghiệp khắc nghiệt.

Giải pháp [**Firewall Palo Alto**](https://viettuans.vn/firewall-palo-alto) cung cấp khả năng hiển thị, kiểm soát và ngăn chặn mối đe dọa nâng cao như: Phần mềm độc hại Malware, virus, xâm nhập trái phép và các mối đe dọa liên tục nâng cao (APT).



\* Tính năng nổi bật

* Ngăn chặn mối đe dọa nâng cao.
* Lọc URL nâng cao.
* Bảo mật dịch vụ tên miền (DNS).
* Bảo mật thiết bị IoT.
* Ngăn ngừa mất dữ liệu doanh nghiệp (DLP).
* Hỗ trợ xử lý lên tới 245 triệu phiên IPv4 IPv6.
* Cơ chế phát hiện ngăn chặn lưu lượng độc hại IPS (Intrusion Prevention System) giúp phát hiện và ngăn chặn các lưu lượng độc hại có thể là rủi ro của các cuộc tấn công mạng, bao gồm cả các cuộc tấn công zero-day, virus, mã độc.

\* Ưu điểm

* Cung cấp khả năng quản lý toàn diện hạ tầng mạng, bao gồm tất cả các thiết bị đầu cuối IoT và các thiết bị được kết nối khác.
* Cung cấp khả năng triển khai trên các môi trường vật lý, ảo hóa, container và đám mây.
* Cung cấp nhiều loại sản phẩm cho các quy mô kinh doanh khác nhau, từ doanh nghiệp nhỏ đến doanh nghiệp lớn.
* Bảng điều khiển tập trung và bảng điều khiển quản lý dễ điều hướng.
* **Fortinet FortiGate:**

Fortinet cũng là 1 trong những hãng bảo mật hàng đầu thế giới, cung cấp nhiều sản phẩm Firewall khác nhau cho các quy mô tổ chức khác nhau, từ văn phòng tại nhà đến các doanh nghiệp lớn.

Dòng sản phẩm Firewall Fortinet FortiGate 7000 (FG-7121F, FG-7081F, FG-7081F-2, FIM-7921F, FIM-7941F và FPM-7620F) được đánh giá cao bởi các chuyên gia trong ngành cũng như khách hàng doanh nghiệp bởi hiệu suất bảo mật Top đầu trong ngành. FortiGate FG-7000 được thiết kế cho các tổ chức có lưu lượng mạng cao và phải quản lý cơ sở hạ tầng mạng lớn.

Dòng Firewall thế hệ mới FortiGate phục vụ cho nhiều kịch bản triển khai khác nhau với sự hỗ trợ của công nghệ AI/ML. Firewall Fortinet cung cấp hiệu suất bảo vệ tại các cơ sở doanh nghiệp đa chi nhánh, triển khai bảo mật siêu quy mô cho các trung tâm dữ liệu, cung cấp khả năng phân đoạn mạng, tích hợp các biện pháp bảo vệ đám mây công cộng và riêng tư, cũng như mở rộng khả năng bảo vệ cho người dùng từ xa với mô hình Secure Access Service Edge (SASE).

[**Firewall Fortinet**](https://viettuans.vn/firewall-fortinet) cấp doanh nghiệp được trang bị Bộ xử lý bảo mật (SPU) với băng thông xử lý lên tới 520Gbps. Bộ xử lý mạng Network Processor NP7 và CP9 (Bộ xử lý nội dung 9) mới nhất. Vì vậy, không bao giờ xảy ra bất kỳ tình trạng giật lag trên các mẫu Firewall của Fortinet.



\* Tính năng nổi bật:

* Bảo vệ toàn bộ hệ thống CNTT, IoT và OT khỏi lỗ hổng bảo mật và các hình thức tấn công dựa trên thiết bị đầu cuối.
* Hộp cát nội tuyến, thử nghiệm, phân tích mẫu độc hại trong 1 container độc lập. Tăng cường hiệu quả và khả năng phát hiện các cuộc tấn công Zero-day chưa được xác định.
* FortiGuard Web and Video Filtering Service: Áp dụng bộ lọc thông minh vào việc quản lý truy cập vào các trang web có nội dung bị cấm hay không phù hợp.
* FortiGuard Advanced Malware Protection: Tổng hợp của những công nghệ phát hiện, tiêu diệt, ngăn chặn các loại hình tấn công bằng virus, malware, botnet. Cơ sở dữ liệu signature của các cuộc tấn công sẽ được cập nhật thường xuyên, đảm bảo tính sẵn sàng và độ tin cậy của hệ thống bảo mật doanh nghiệp.
* FortiGuard Antispam Service: Thư rác sẽ không còn là hiểm họa tiềm ẩn của các cuộc tấn công mạng khi doanh nghiệp của bạn sử dụng dịch vụ FortiGuard Antispam Service.
* Mô hình xác thực ZTNA, xác minh quyền truy cập đối với tất cả người dùng doanh nghiệp.
* **ForcePoint:**

Forcepoint cung cấp giải pháp Firewall thế hệ tiếp theo (NGFW) đáng tin cậy đã nhanh chóng thu hút được sự chú ý của các doanh nghiệp. Giải pháp này có các tính năng nâng cao như SD-WAN bảo mật tích hợp cho phép các tổ chức áp dụng kiến ​​trúc Secure Access Service Edge (SASE), cập nhật chính sách bảo mật thống nhất tự động và dễ dàng triển khai, cấu hình và sử dụng. [**Firewall Forcepoint**](https://viettuans.vn/firewall-forcepoint) được thiết kế để có khả năng mở rộng và tùy chỉnh cao, cho phép cập nhật và thay đổi nhanh chóng khi cần thiết.

Firewall Forcepoint NGFW cung cấp một số tính năng chính, bao gồm hỗ trợ xác thực 2 bước hoặc xác thực đa yếu tố (2FA/MFA) cho người dùng cuối từ xa. Giải pháp Firewall của ForcePoint cung cấp khả năng quản lý tập trung trên 1 bảng điều khiển duy nhất số lượng lớn thiết bị Firewall vật lý cũng như đám mây, ảo hóa

Ngoài ra, Forcepoint NGFW tích hợp với Secure Access Service Edge (SASE), cung cấp giải pháp Secure SD-WAN, kết nối trang web với Security Service Edge qua VPN mã hóa GRE hoặc IPsec, cũng như mô hình xác thực Zero Trust Network Access (ZTNA) tích hợp sẵn.

* **Cisco:**

Firewall bảo mật của Cisco kết hợp các khả năng của Firewall với các tính năng bảo mật nâng cao để bảo vệ mạng khỏi nhiều mối đe dọa khác nhau, bao gồm truy cập trái phép, phần mềm độc hại và vi phạm dữ liệu.

Các giải pháp Firewall của Cisco được hỗ trợ đắc lực bởi Cisco Talos - Một nhóm nghiên cứu thông tin về các mối đe dọa đã đang và chưa xác định. Sự hợp tác này cho phép các giải pháp [**Firewall Cisco**](https://viettuans.vn/firewall-cisco) luôn nhận được các bản cập nhật thông tin về mối đe dọa theo thời gian thực, nâng cao khả năng xác định và ngăn chặn các mối đe dọa không xác định. Vì vậy, giảm thiểu tối đa rủi ro của thảm họa Zero-day nhắm vào doanh nghiệp.

Firewall bảo mật của Cisco có thể được quản lý tập trung thông qua nền tảng Firewall Management Center (FMC). Bảng điều khiển quản lý tập trung này cung cấp giao diện thống nhất để cấu hình, giám sát và báo cáo, đơn giản hóa việc quản trị nhiều thiết bị Firewall trong mạng.

\* Tính năng nổi bật

* IPS để bảo vệ chống lại các mối đe dọa đã biết.
* Lọc web.
* Chống virus, malware, ransomware cùng nhiều hình thức tấn công khác.
* Kiểm soát quyền truy cập users
* Phân đoạn mạng.
* Quản lý tập trung.

\* Ưu điểm

* Cung cấp khả năng triển khai đa kịch bản doanh nghiệp và kiểm soát toàn diện hệ thống mạng.
* Công cụ có khả năng mở rộng cao.

# **TÀI LIỆU THAM KHẢO**

[1] <https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall>

[2] <https://viettuans.vn/thiet-bi-tuong-lua-firewall>

[3] <https://doc.edu.vn/tai-lieu/tieu-luan-tim-hieu-va-xay-dung-he-thong-firewall-ma-nguon-mo-su-dung-smoothwall-7436/>

[4] <https://tailieu.vn/doc/tim-hieu-ve-tuong-lua-tuong-lua-la-gi--1242779.html>

[5] https://en.wikipedia.org/wiki/Firewall\_(computing)