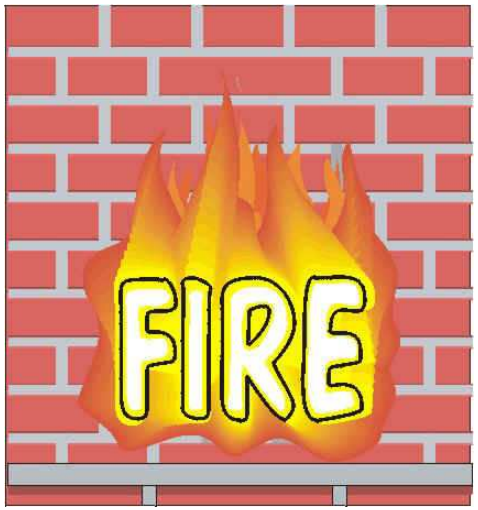
## Chương 7

# Tường lửa (Firewall)

- Khái niệm
- Phân loại
- Cấu hình
- Các hệ thống tín nhiệm

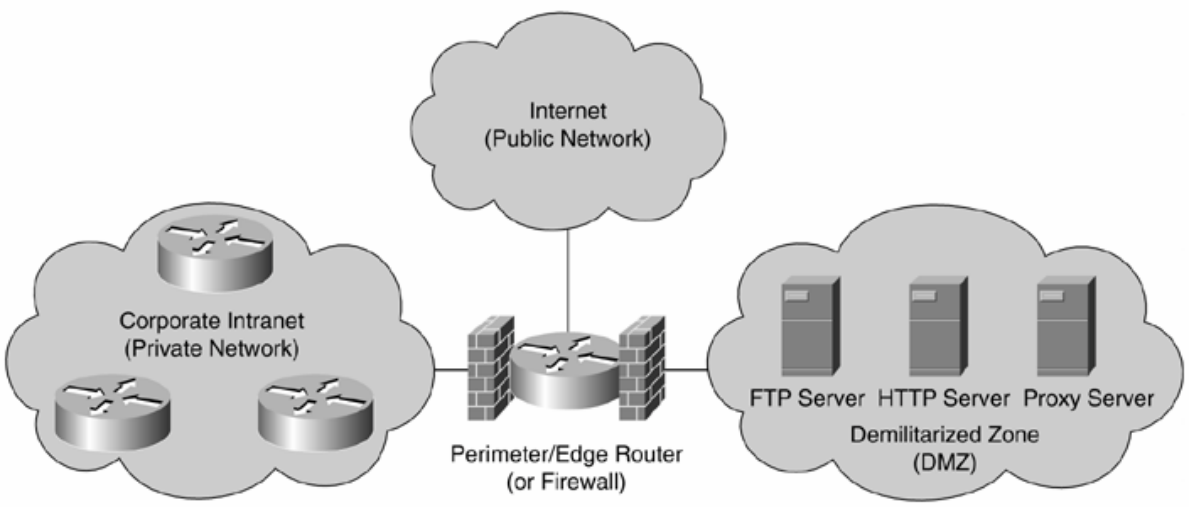


# Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan các loại tường lửa và cách thức sử dụng tường lửa.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Trình bày được tường lửa là gì, vị trí của tường lửa trong mô hình mạng máy tính.
  - Mô tả được các đặc điểm của tường lửa
  - Phân biệt được các loại tường lửa.
  - Hiểu được nguyên lý cấu hình tường lửa.
  - Trình bày được khái niệm hệ thống tín nhiệm và ứng dụng của chúng trong việc ngăn ngừa các tấn công bằng mã độc hại.

# Khái niệm

- Khái niệm



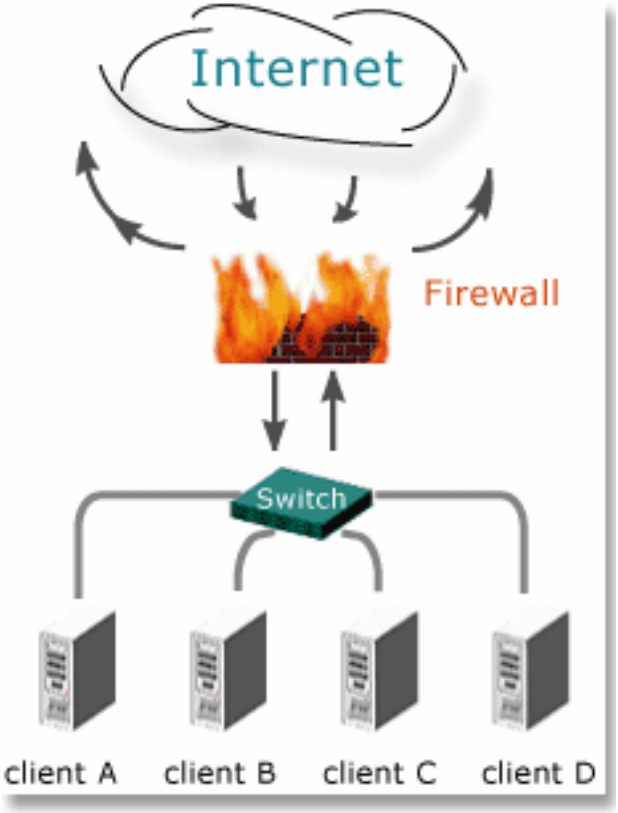

**Firewall** có thể là :
- 1 router
- 1 PC thực thi phần mềm chuyên dụng
- Tập hợp nhiều thiết bị phần cứng.

- Firewall được đặt ở giữa mạng nội bộ và mạng ngoài (Internet).
- Firewall sử dụng điều khiển truy cập để bảo đảm tính an toàn cho mạng nội bộ.

**Mục tiêu thiết kế**
- Tất cả lưu thông từ ngoài vào trong và ngược lại đều phải đi qua Firewall.
- Chỉ có những lưu thông hợp lệ mới được phép đi qua
- Ngăn chặn các xâm nhập vào mạng.

# Khái niệm

- Các kỹ thuật sử dụng trong Firewall




**4 kỹ thuật Firewall sử dụng**:

• **Điều khiển dịch vụ**: xác định các loại dịch vụ mạng nào có thể được truy cập vào hoặc ra, lọc lưu thông mạng dựa theo địa chỉ IP và cổng.
• **Điều khiển hướng**: xác định hướng truy cập cho phép của từng loại dịch vụ.
• **Điều khiển người dùng**: dựa vào kết quả chứng thực để xác định đối tượng có thể truy cập.
• **Điều khiển ứng xử**: xác định những dịch vụ đặc biệt được sử dụng như thế nào. VD: cho phép truy cập từ ngoài vào 1 phần thông tin nào đó trên web server.

# Khái niệm

- Đặc điểm của Firewall


**Khả năng của Firewall**

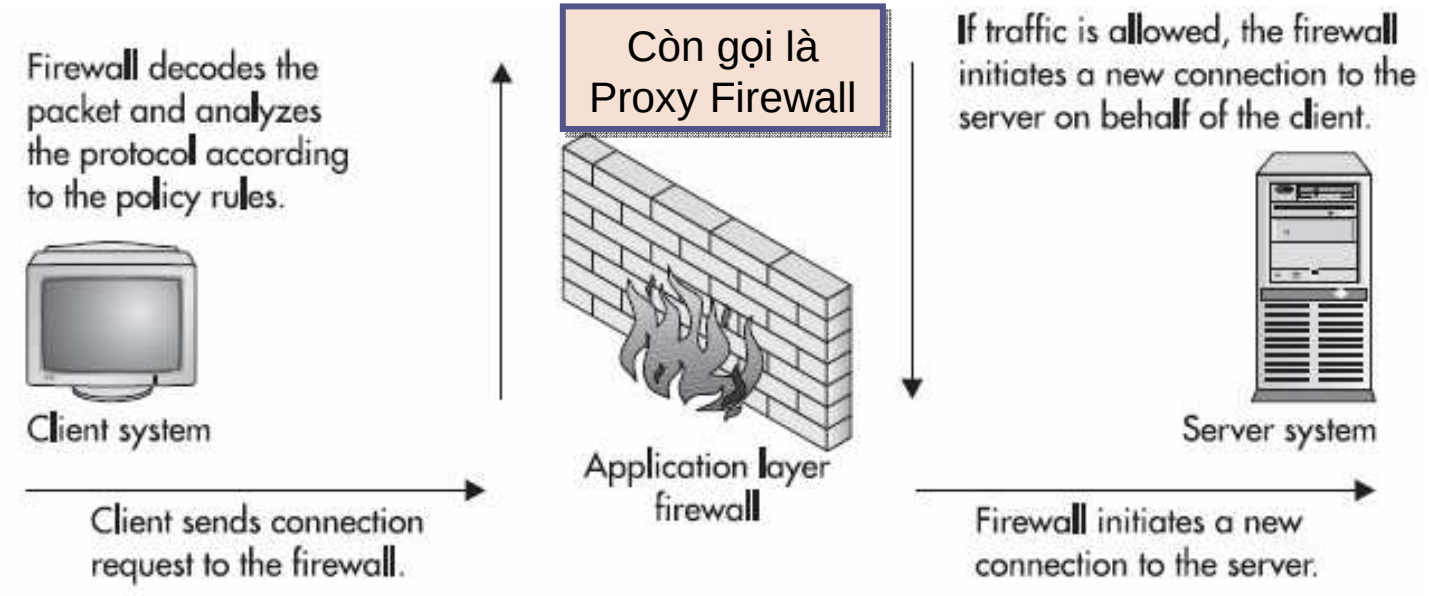
• Là điểm chặn những kẻ trái phép ở ngoài mạng riêng của tổ chức, ngăn cấm những dịch vụ nguy hiểm, bảo vệ mạng trước các tấn công giả mạo và tấn công vạch đường.
• Là nơi để giám sát và cảnh báo các sự kiện bảo mật trong mạng.
• Cung cấp nền cho các chức năng trên Internet như: NAT, kiểm soát, ghi log.
• Có thể sử dụng để cài đặt VPN.

**Giới hạn của Firewall**

• Không thể ngăn chặn các tấn công không đi qua Firewall như tấn công thông qua đường truy xuất Dialup.
• Không thể bảo vệ trước các mối nguy hại từ bên trong.
• Không thể bảo vệ trước tấn công của virus vào dữ liệu hay phần mềm.

# Phân loại

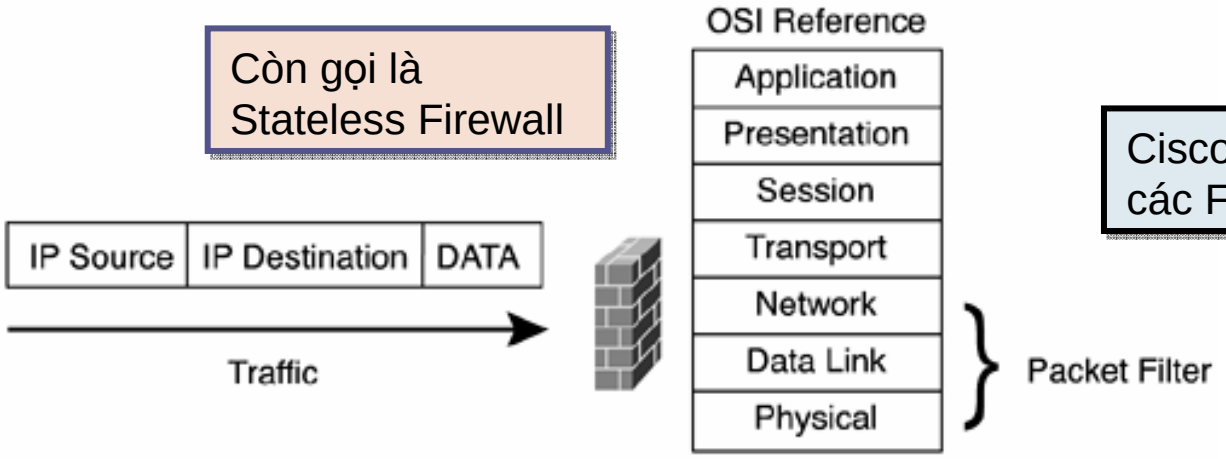
- Firewall tầng ứng dụng (application layer firewall)




• Thường được cấu hình chỉ cho phép sử dụng các dịch vụ cơ bản như Web, FTP, SMTP, Telnet, …
• Che dấu địa chỉ nguồn yêu cầu từ mạng nội bộ.
• Đa số là dạng ứng dụng => chậm, không thích hợp với mạng lớn.

# Phân loại

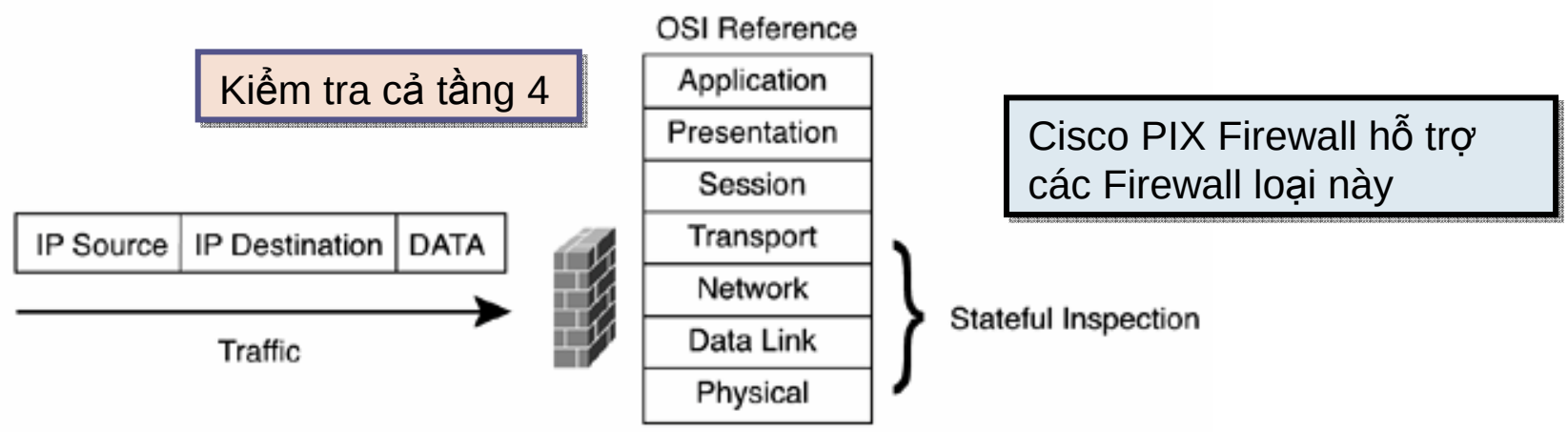
- Firewall lọc gói (paket filtering)




Cài đặt các quy tắc (rule) điều khiển lưu thông mạng dựa theo:
- Địa chỉ IP của nơi gửi
- Địa chỉ IP của nơi nhận

# Phân loại

- Firewall đầy đủ trạng thái (stateful)

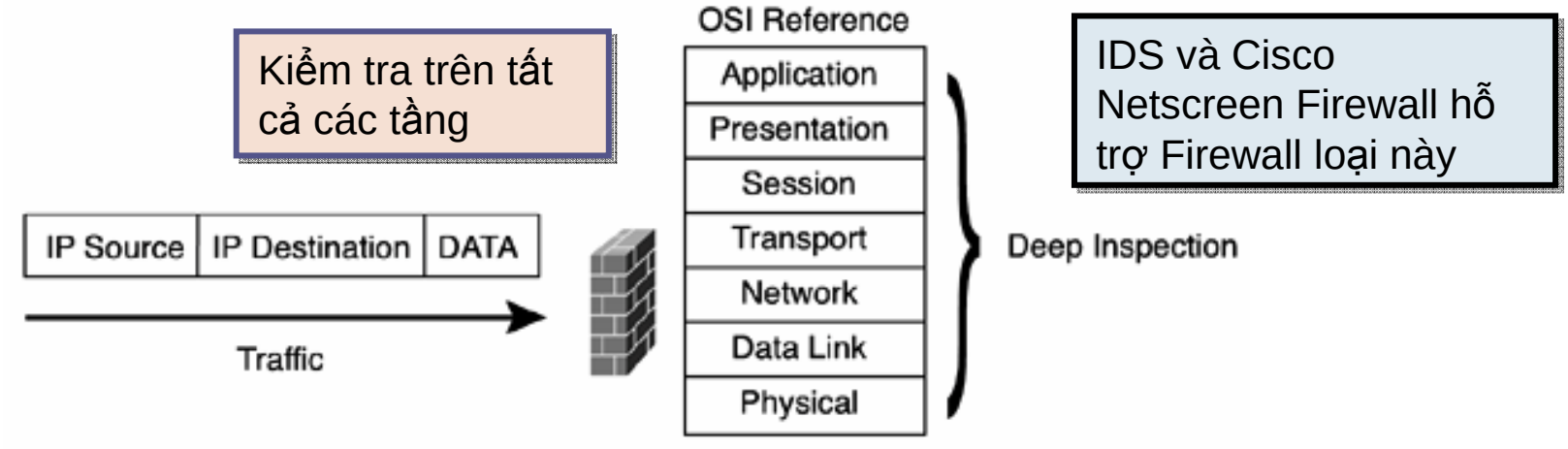



Cài đặt các quy tắc (rule) điều khiển lưu thông mạng dựa theo:
- Địa chỉ IP của nơi gửi
- Địa chỉ IP của nơi nhận
- Cổng của quá trình gửi
- Cổng của quá trình nhận

Một số khác còn cho phép kiểm tra nội dung dữ liệu và tính bất thường của giao thức

# Phân loại

- Firewall duyệt sâu gói tin (deep packet layer)




Tương tự như Stateful packet nhưng bổ sung thêm các tính năng:
- Đảm bảo các gói tin phù hợp với giao thức
- Đảm bảo các gói tin phù hợp với các mô tả chi tiết
- Đảm bảo các gói tin không phải là các phần mềm tấn công
- Đảm bảo tính toàn vẹn của dữ liệu truyền đi giữa các thiết bị.

Chống tấn công DoS và chống virus

# Cấu hình

- Các quy tắc – Packet filter firewall

| Action | Our host | Port | Their host | Port | Comment |
|---|---|---|---|---|---|
| Block | * | * | 203.1.2.3 | * | Mọi truy cập từ 203.1.2.3 đều bị cấm |
| Allow | Server1 | 25 | * | * | Cho phép truy cập từ ngoài vào Server1 với dịch vụ SMTP |
| Block | * | * | * | * | Default |

Đây là chính sách mặc nhiên, thường được thêm vào cuối bảng quy tắc
=> Ngoài các quy tắc định nghĩa phía trên, mọi thứ truy cập khác đều bị cấm

# Cấu hình

- Các quy tắc – Packet filter firewall

| Action | Our host | Port | Their host | Port | Comment |
|---|---|---|---|---|---|
| Allow | * | * | * | 25 | Nối kết đến SMTP Server ở ngoài |

Cho phép tất cả máy tính bên trong mạng cục bộ có thể gửi mail trực tiếp đến các SMTP Server ở mạng bên ngoài.

Có thể bị Hacker lợi dụng bằng cách giả mạo 1 ứng dụng cổng 25 để kết nối ngược lại các máy tính bên trong.

# Cấu hình

- Các quy tắc – Packet filter firewall

| Action | Source | Source Port | Dest | Dest Port | Flag | Comment |
|---|---|---|---|---|---|---|
| Allow | Our hosts | * | * | 25 | | Nối kết đến SMTP Server ở ngoài |
| Allow | * | 25 | * | * | ACK | Cho phép các trả lời từ SMTP Server gửi lại |

Thay đổi cách định nghĩa các quy tắc (tránh tạo lỗ hổng cho khai thác):
- Các máy tính bên trong mạng có thể gửi mail trực tiếp đến các SMTP Server.
- Mọi trả lời từ các SMTP Server đều cho phép đi vào mạng.

# Cấu hình

- Các quy tắc – Packet filter firewall

Một ví dụ thực tế về các quy tắc tại Firewall

| | Source Address | Source Port | Destination Address | Destination Port | Action | Description |
|---|---|---|---|---|---|---|
| 1 | Any | Any | 192.168.1.0 | > 1023 | Allow | Rule to allow return TCP Connections to internal subnet |
| 2 | 192.168.1.1 | Any | Any | Any | Deny | Prevent Firewall system itself from directly connecting to anything |
| 3 | Any | Any | 192.168.1.1 | Any | Deny | Prevent External users from directly accessing the Firewall system. |
| 4 | 192.168.1.0 | Any | Any | Any | Allow | Internal Users can access External servers |
| 5 | Any | Any | 192.168.1.2 | SMTP | Allow | Allow External Users to send email in |
| 6 | Any | Any | 192.168.1.3 | HTTP | Allow | Allow External Users to access WWW server |
| 7 | Any | Any | Any | Any | Deny | "Catch-All" Rule - Everything not previously allowed is explicitly denied |

# Cấu hình

- Các quy tắc – Stateful firewall

Quy định các giao dịch cụ thể nào được sử dụng

| Source Address | Source Port | Destination Address | Destination Port | Connection State |
|---|---|---|---|---|
| 192.168.1.100 | 1030 | 210.9.88.29 | 80 | Established |
| 192.168.1.102 | 1031 | 216.32.42.123 | 80 | Established |
| 192.168.1.101 | 1033 | 173.66.32.122 | 25 | Established |
| 192.168.1.106 | 1035 | 177.231.32.12 | 79 | Established |
| 223.43.21.231 | 1990 | 192.168.1.6 | 80 | Established |
| 219.22.123.32 | 2112 | 192.168.1.6 | 80 | Established |
| 210.99.212.18 | 3321 | 192.168.1.6 | 80 | Established |
| 24.102.32.23 | 1025 | 192.168.1.6 | 80 | Established |