

An toàn mạng máy tính

Chương 2.

Công nghệ tường lửa

Tài liệu tham khảo:

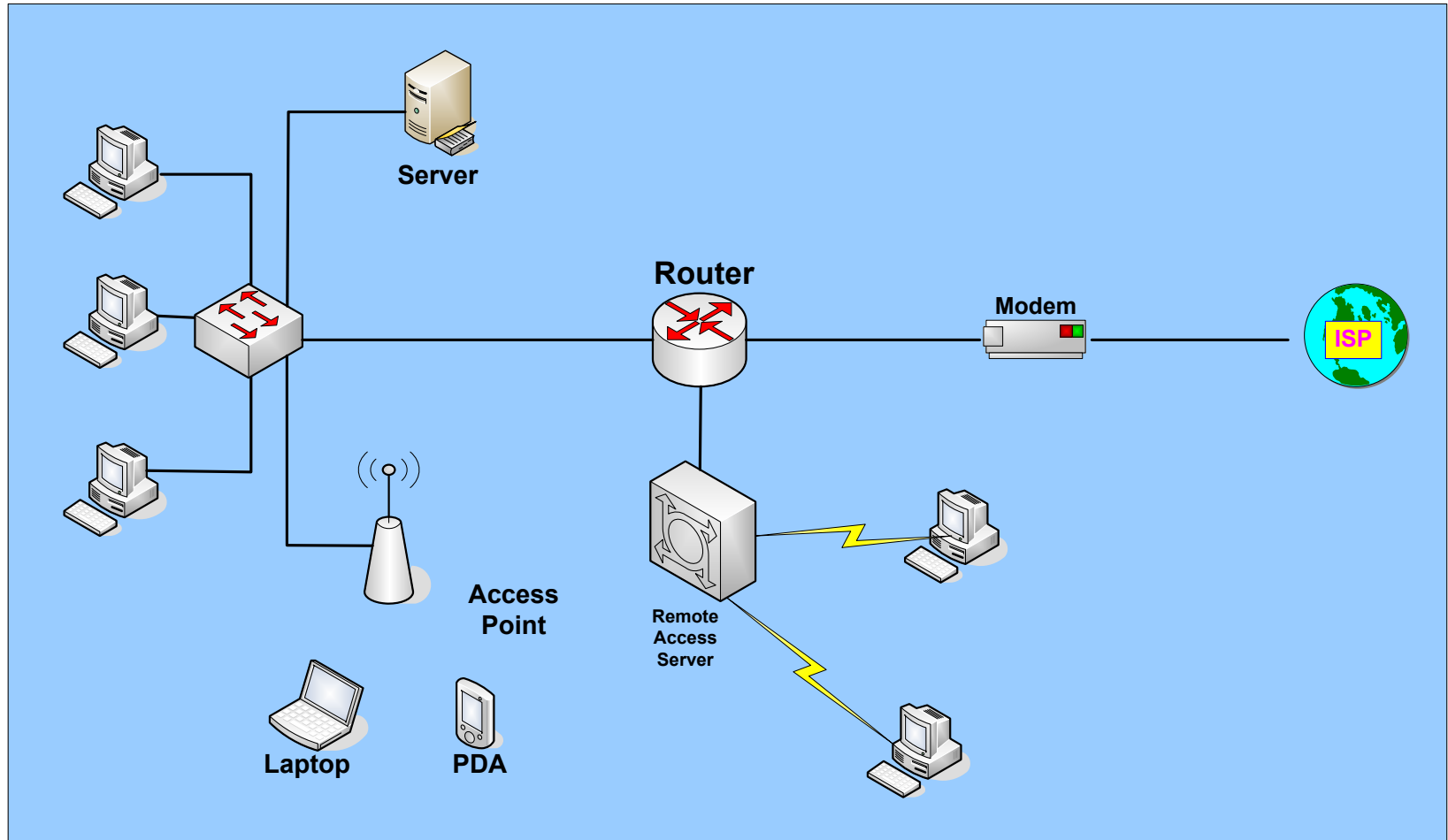
1. *Principles of Information Security*. Michael E. Whitman. 2011.
2. *NIST 800-94. Guide to Intrusion Detection and Prevention Systems*. 2007.
3. *Computer Security Fundamentals*. Chuck Easttom. 2012.
4. *CISSP. All in one*. Shon Harris. Sixth Edition. 2013
5. *Secure Computer and Network Systems*. Nong Ye. 2008.

Nội dung bài giảng:

1. Sơ đồ mạng an toàn
2. Công nghệ tường lửa

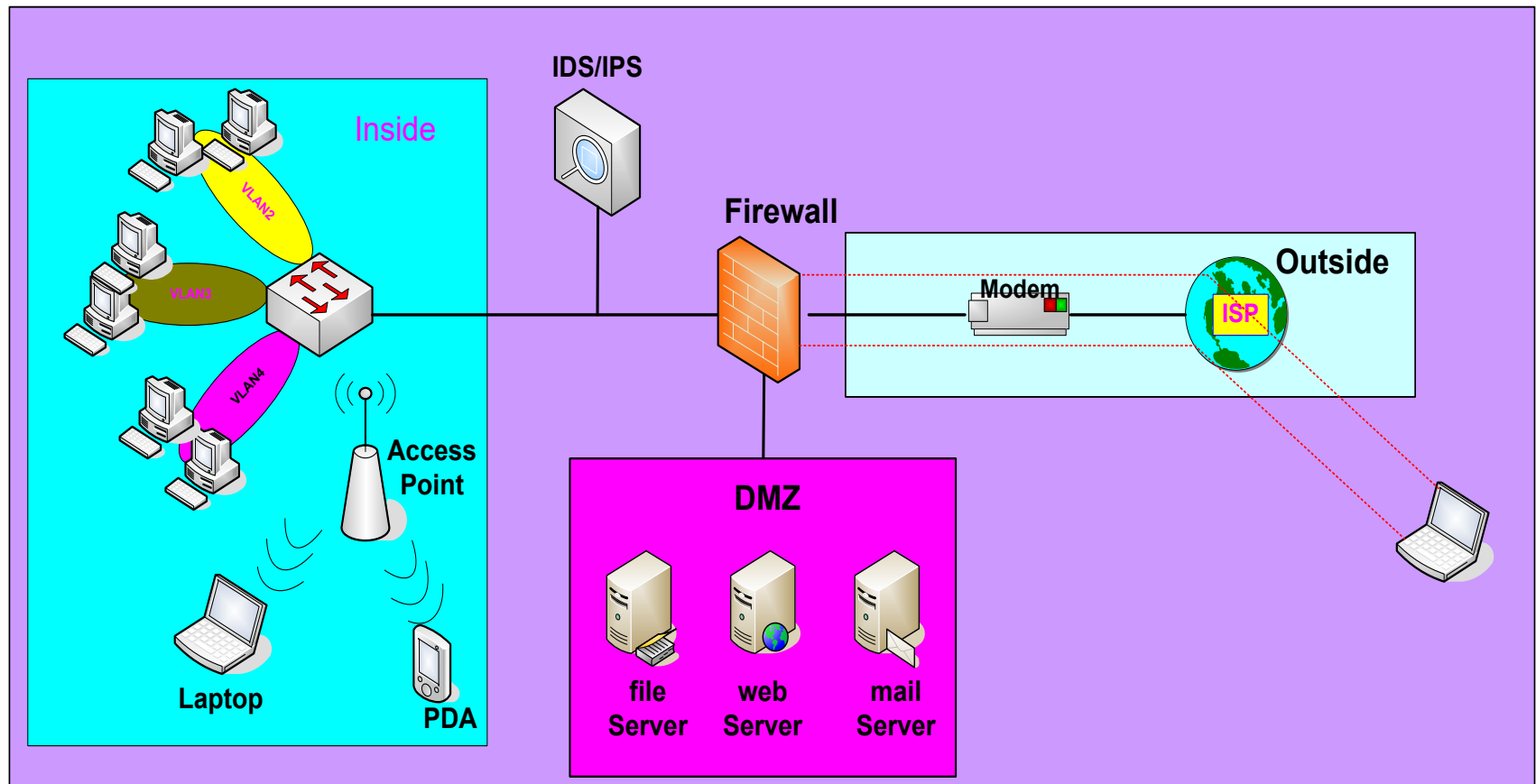
1. Sơ đồ mạng an toàn

Đánh sơ đồ mạng sau:



1. Sơ đồ mạng an toàn

Sơ đồ mạng áp dụng công nghệ an toàn:



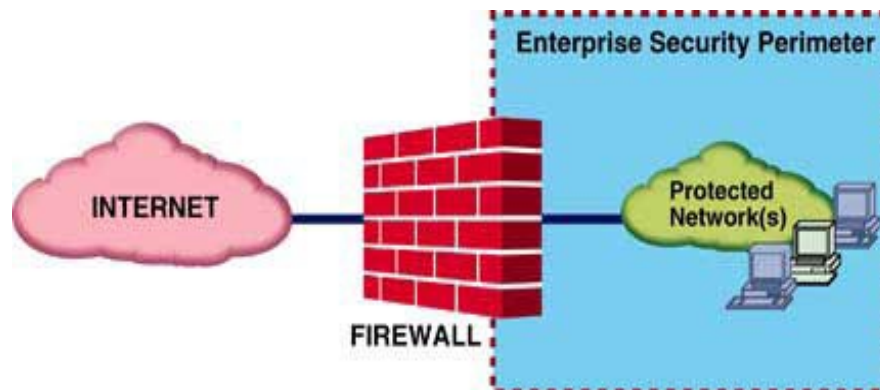


Chương 2. Công nghệ tường lửa

2. Công nghệ tường lửa

Định nghĩa:

Firewall là thành phần tham gia vào mạng máy tính tồn tại dưới dạng phần cứng hoặc phần mềm nằm ở cổng vào ra của mạng.



2. Công nghệ tường lửa

Chức năng:

Chức năng chính của tường lửa là điều khiển, kiểm soát truy cập.

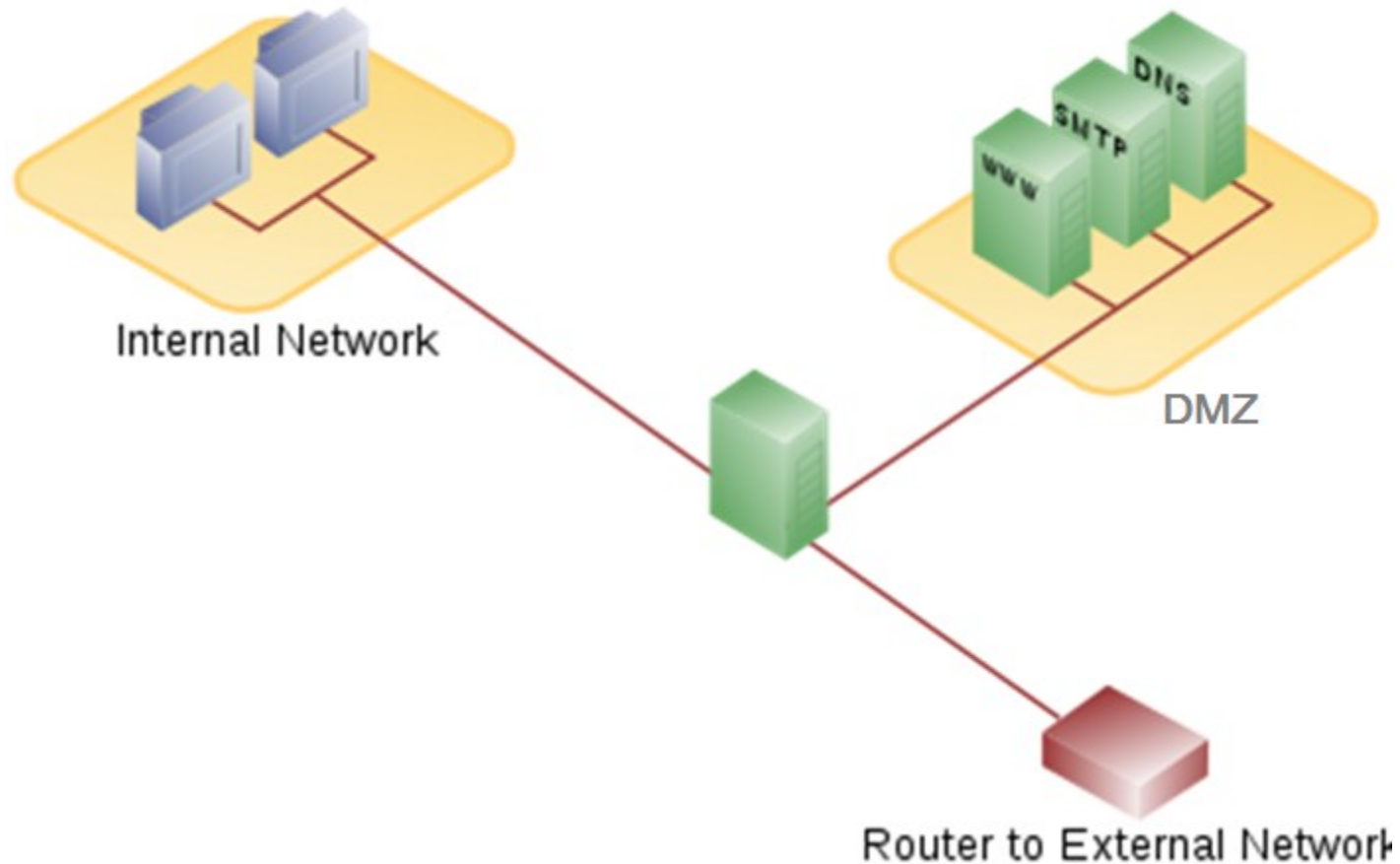
- Kiểm soát dịch vụ (service control)
- Kiểm soát hướng (direction control)
- Kiểm soát người dùng (user control)
- Kiểm soát hành vi (behaviour control)

2. Công nghệ tường lửa

■ Phân thành các vùng (zones)

- Intranet (inside): trusted
- Extranet (outside): un-trusted
- DMZ – De-Militerized Zone

2. Công nghệ tường lửa



2. Công nghệ tường lửa

Phân loại tường lửa

Có nhiều cách phân loại tường lửa khác nhau:

- a. Phân loại theo nhà sản xuất*
- b. Phân loại theo phạm vi sử dụng*
- c. Phân loại theo mô hình tầng mạng*
- d. Phân loại theo trạng thái*

2. Công nghệ tường lửa

Phân loại theo nhà sản xuất:

Mỗi một nhà sản xuất thì họ có các sản phẩm tường lửa khác nhau, và mức độ bảo vệ cho hệ thống mạng cũng khác nhau.

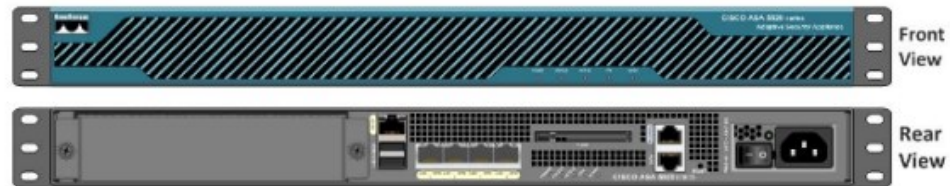
■ Tường lửa cứng:

- ✓ Là loại tường lửa được sản xuất thành sản phẩm chuyên dụng.
- ✓ Người quản trị chỉ cần lắp ráp và cấu hình cho nó.
- ✓ Một số tường lửa cứng điển hình: Check Point, Juniper, Cisco...

2. Công nghệ tường lửa

Cisco ASA 5520

Cisco ASA 5520



Check Point



Juniper



2. Công nghệ tường lửa

■ Tường lửa mềm:

- ✓ Là sản phẩm tường lửa được đóng gói thành phần mềm và cần phải có máy chủ và hệ điều hành của hãng thứ ba để cài đặt.
- ✓ Một số tường lửa mềm điển hình:
 - ISA hoặc Forefont (TMG) của hãng Microsoft,
 - ZoneAlarm của hãng CheckPoint,
 - Proventia Network của hãng IBM.
 - Iptables tren Linux
 - PfSense 2.4.0

2. Công nghệ tường lửa

Phân loại theo phạm vi sử dụng:

■ Tường lửa cá nhân:

- ☐ Là loại tường lửa được cài đặt tại máy tính cá nhân.
- ☐ Có chức năng kiểm soát luồng thông tin vào ra ngay tại máy tính cá nhân.

■ Tường lửa mạng:

- ☐ Là loại tường lửa hoạt động trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các vùng mạng DMZ.

2. Công nghệ tường lửa

Phân loại theo mô hình tầng mạng:

- Tầng mạng và giao vận:
 - Là loại tường lửa hoạt động ở tầng mạng trong mô hình OSI.
- Tầng phiên:
 - Tường lửa cổng vòng.
- Tầng ứng dụng:
 - Tường lửa cổng ứng dụng. (Proxy)



































2. Công nghệ tường lửa

Phân loại theo trạng thái:

- Tường lửa có trạng thái (Stateful firewall).
 - Firewall loại này ghi nhớ trạng thái của các kết nối tại mức mạng và phiên nhờ ghi lại các thông tin thiết lập phiên mà được pass thông qua Firewall.
 - Firewall lưu trạng thái vào state table sau khi kết nối được thiết lập.
- Tường lửa phi trạng thái (Stateless firewall).
 - Lọc gói tin dựa vào các giá trị tĩnh: IP, port nguồn và đích.

2. Công nghệ tường lửa

Luật của tường lửa:

Firewall Policy						
O... ^	Name	Action	Protocols	From / Listener	To	Condition
 1	Allow DNS Forwarding	 Allow	 DNS	 Internal DNS Server	 External	 All Users
  2	Allow POP3 / SMTP	 Allow	 POP3  SMTP	 Internal	 External	 All Users
 3	BLOCKED URLs	 Deny	 All Outbound Traffic	 Internal	 Blocked URLs	 All Users
  4	Allow HTTP/HTTPS	 Allow	 HTTP  HTTPS	 Internal	 External	 All Users
 L... Default rule		 Deny	 All Traffic	 All Networks (and Lo...	 All Network...	 All Users

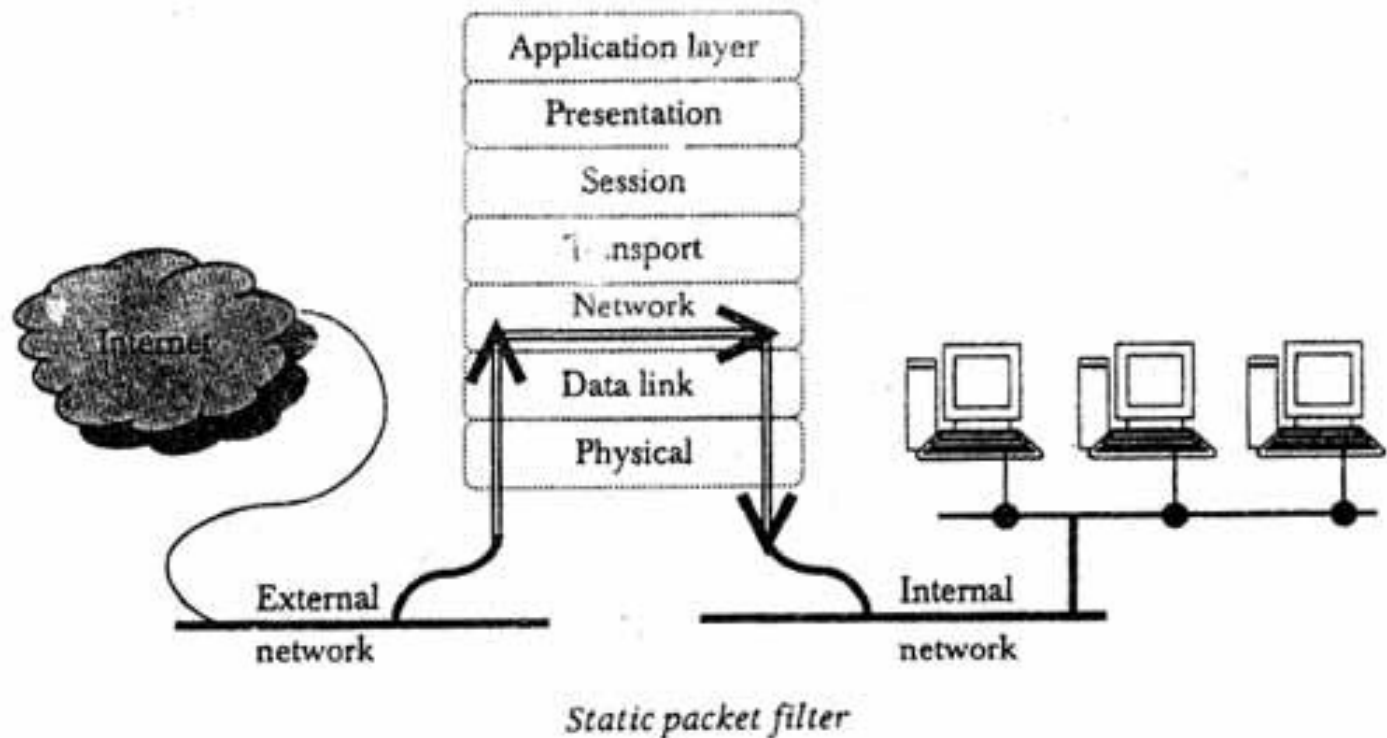


Một số công nghệ tường lửa điển hình:

- 1. Tường lửa lọc gói**
- 2. Tường lửa cổng chuyển mạch**
- 3. Tường lửa ứng dụng**

2.1 Tường lửa lọc gói

Hoạt động chặt chẽ theo mô hình OSI:



2.1 Tường lửa lọc gói

■ Nguyên lý

- Kiểm tra gói tin để quyết định xem các gói tin đó có thỏa mãn các luật của bộ lọc hay không.
- Bộ lọc gói tin cho phép (thỏa mãn) hay từ chối (không thỏa mãn) mỗi gói tin mà nó nhận được.

2.1 Tường lửa lọc gói

Các luật lọc này dựa trên thông tin nào ?

- Dựa trên các trường trong phần đầu của IP, TCP hay UDP
 - Địa chỉ IP xuất phát (IP source address)
 - Địa chỉ IP nơi nhận (IP destination address)
 - Giao thức sử dụng (TCP, UDP, ICMP...)
 - Cổng nguồn TCP/UDP
 - Cổng đích TCP/UDP
 - Giao diện packet đến
 - Giao diện packet đi

2.1 Tường lửa lọc gói

- Bảng luật chứa danh sách các rules, nếu thông tin trong gói tin trùng với rule, thì rule đó được áp dụng và xác định gói tin đó được **chuyển tiếp** hay **ngăn chặn**.
- Nếu không trùng với bất kỳ rule nào, thì rule mặc định được áp dụng.
 - Thường thì có hai chính sách cho luật mặc định:
 - mặc định = chuyển tiếp
 - hoặc mặc định = loại bỏ.
- Luật được duyệt từ trên xuống, mức ưu tiên giảm dần.

2.1 Tường lửa lọc gói

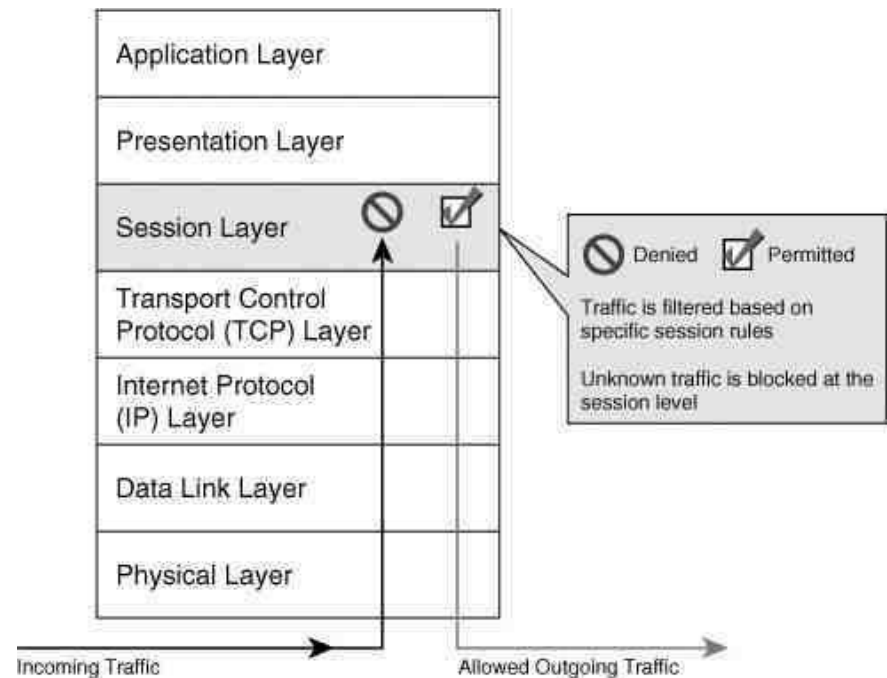
- Ví dụ: Tường lửa cho phép DNS

```
#iptables -A OUTPUT -p udp -o eth0 --dport 53 --sport  
1024:65535 -j ACCEPT
```

```
#iptables -A INPUT -p udp -i eth0 --sport 53 --dport 1024:65535  
-j ACCEPT
```

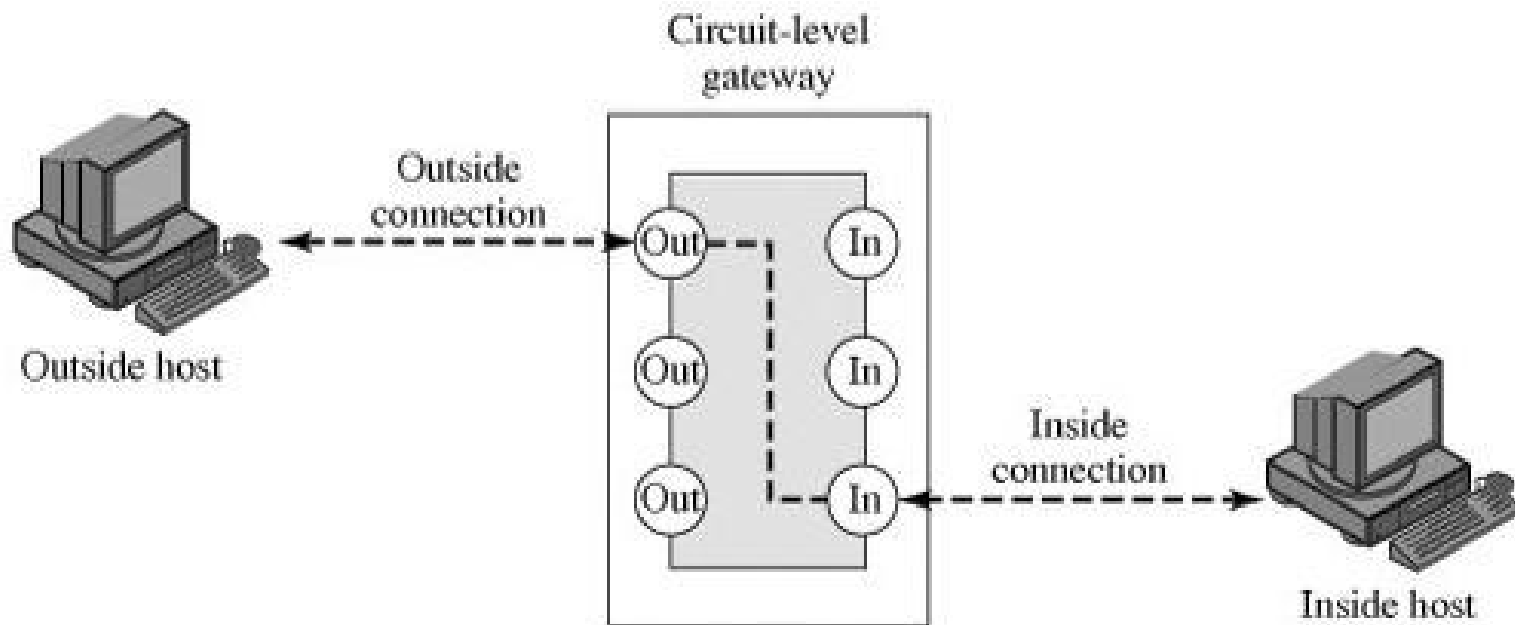

2.2 Tường lửa cổng chuyển mạch

- Hoạt động ở tầng phiên trong OSI
- Giám sát bắt tay giữa các gói tin TCP vào/ra để xác định phiên làm việc có hợp lệ hay không.



2.2 Tường lửa cổng chuyển mạch

- Nguyên lý hoạt động: Không cho phép thực hiện kết nối end – to – end.



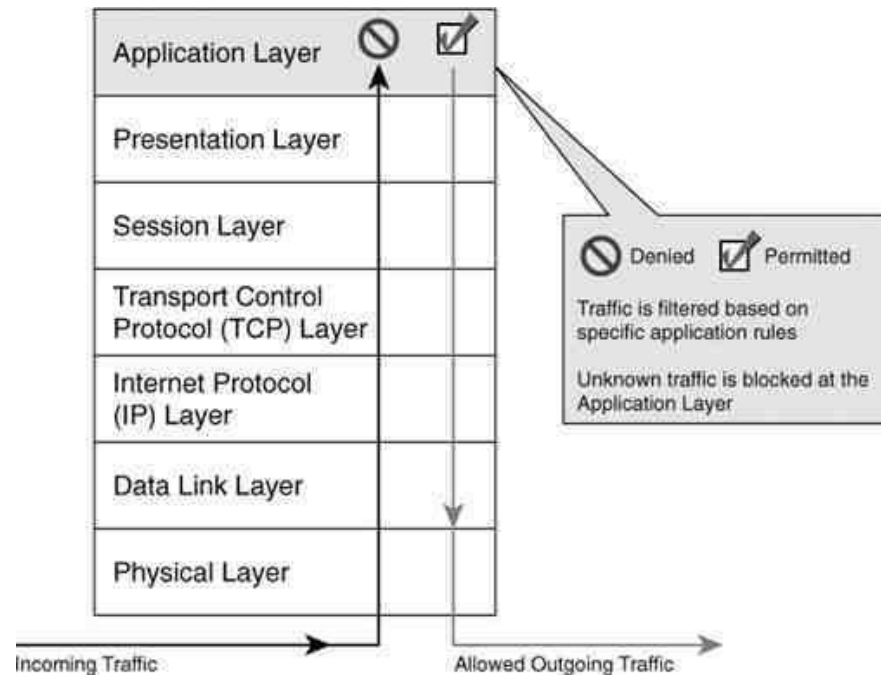
2.2 Tường lửa cổng chuyển mạch

Tiến trình thực hiện:

- Máy bên trong yêu cầu một dịch vụ, cổng chuyển mạch chấp nhận yêu cầu đó.
- Thay mặt máy bên trong, cổng chuyển mạch mở kết nối đến máy bên ngoài và giám sát chặt chẽ quá trình bắt tay TCP. Quá trình bắt tay liên quan đến việc trao đổi gói tin chứa cờ (SYN hay ACK).
- Cổng chuyển mạch xác thực máy bên trong và máy bên ngoài là thành phần một phiên làm việc, cổng sao chép và chuyển tiếp dữ liệu giữa hai kết nối.
- Cổng duy trì một bảng thiết lập kết nối, dữ liệu được phép đi qua nếu thuộc một trong các phiên làm việc có trong bảng.
- Khi phiên làm việc kết thúc, cổng chuyển mạch xóa bản ghi kết nối của phiên làm việc đó.
- Bảng kết nối: Session ID, Trạng thái (handshake, established), sequence number ...

2.3 Tường lửa cổng ứng dụng

- Hoạt động ở tầng ứng dụng.
- Thiết kế nhằm tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào/ra hệ thống mạng.

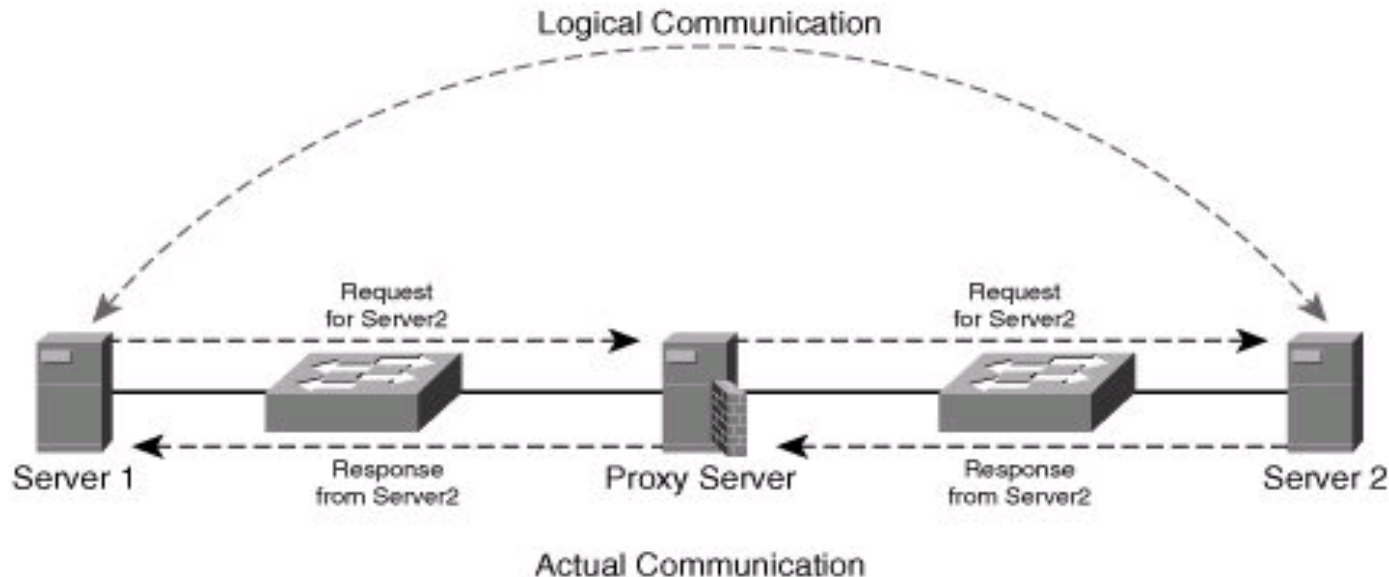


2.3 Tường lửa cổng ứng dụng

Nguyên lý hoạt động:

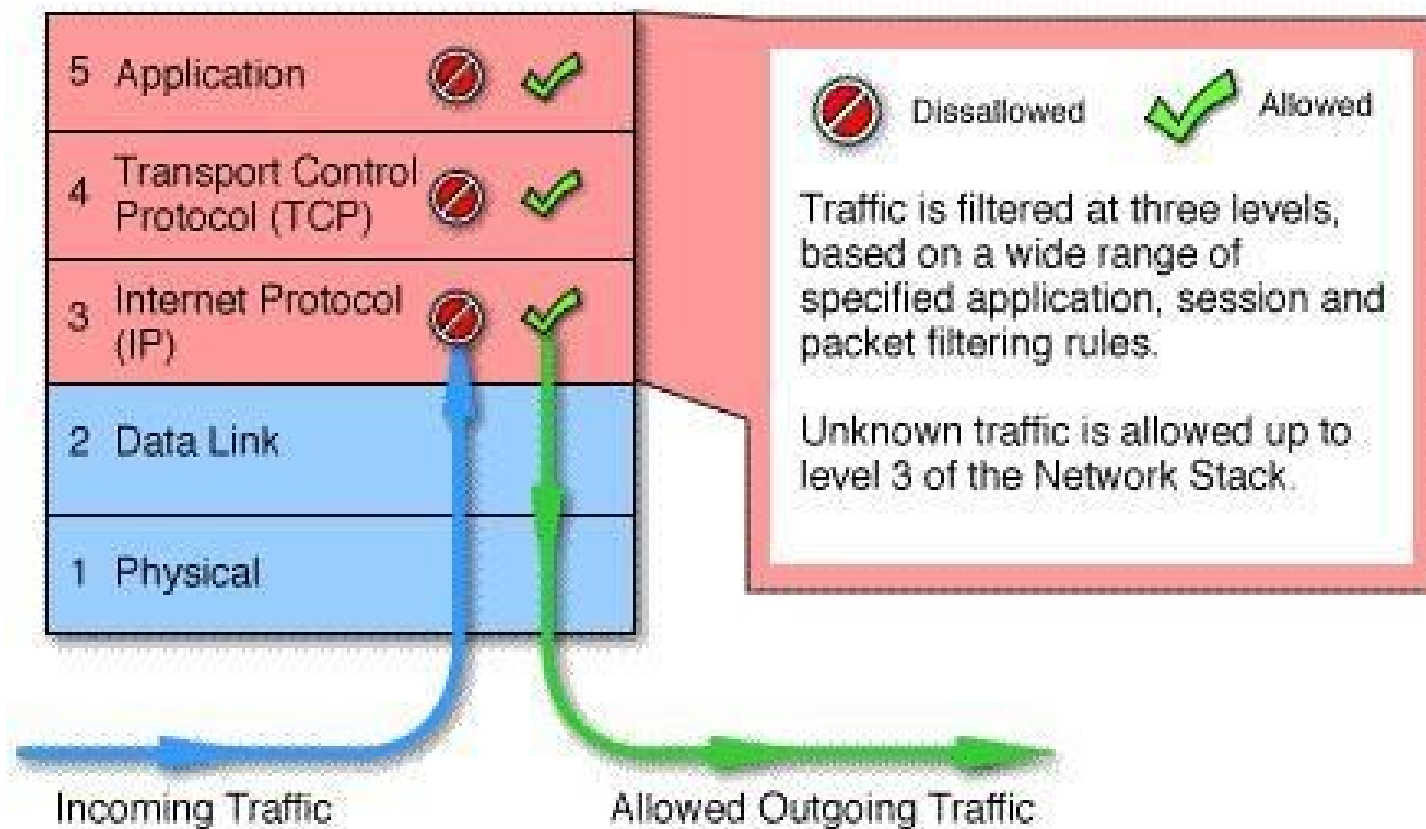
- Dựa trên các dịch vụ đại diện (Proxy service).
- Proxy service là các chương trình đặc biệt cài trên gateway cho từng ứng dụng.
- Quy trình kết nối sử dụng dịch vụ thông qua cổng ứng dụng diễn ra theo 5 bước.

2.3 Tường lửa cổng ứng dụng

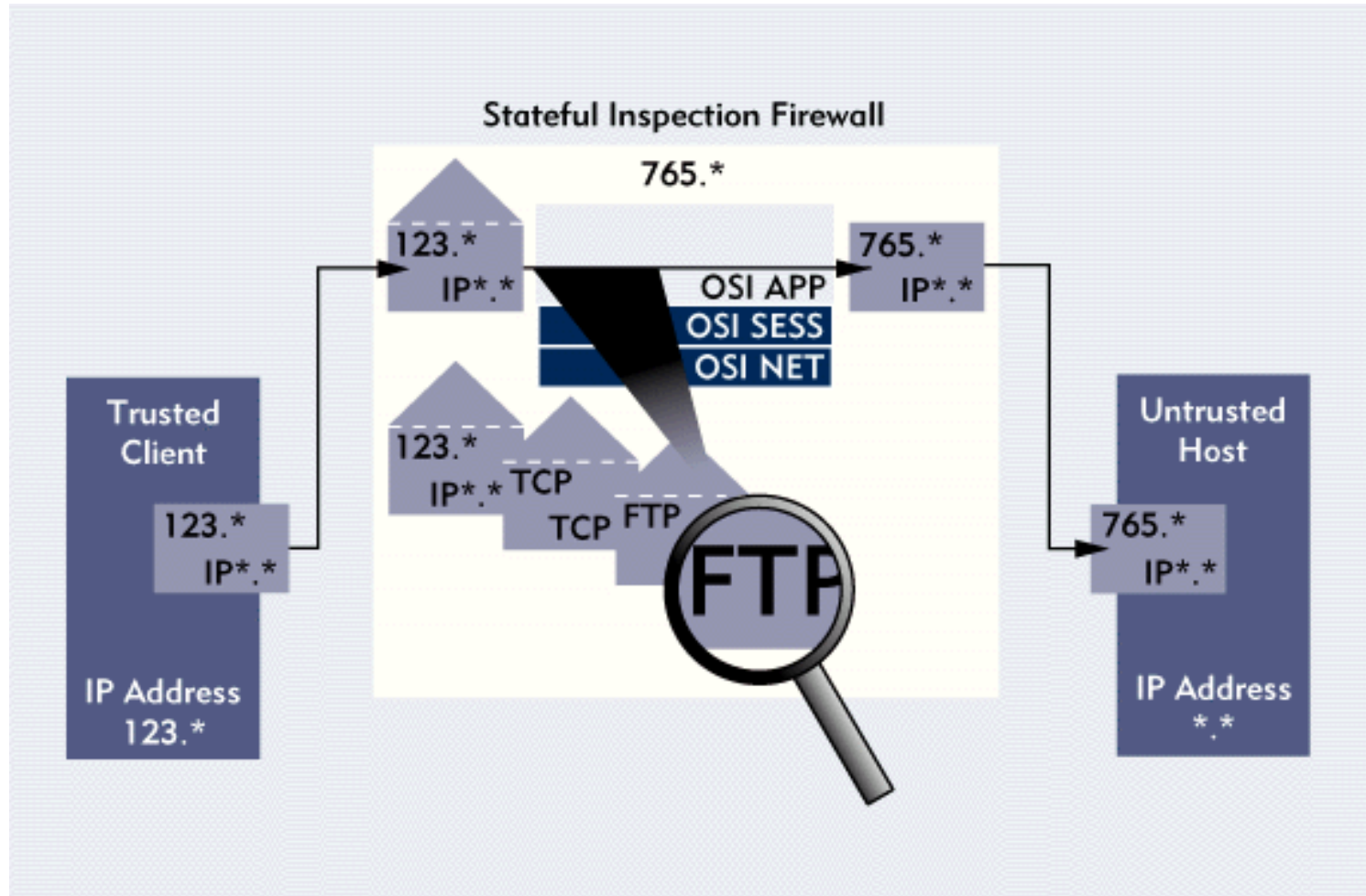


- **Bước 1:** Máy trạm gửi yêu cầu tới máy chủ ở xa đến cổng ứng dụng.
- **Bước 2:** Cổng ứng dụng xác thực người dùng. Nếu xác thực thành công chuyển sang bước 3, ngược lại quá trình kết thúc.
- **Bước 3:** Cổng ứng dụng chuyển yêu cầu máy trạm đến máy chủ ở xa.
- **Bước 4:** Máy chủ ở xa trả lời chuyển đến cổng ứng dụng.
- **Bước 5:** Cổng ứng dụng chuyển trả lời của máy chủ ở xa đến máy trạm.

2.4 Tường lửa trạng thái



2.4 Tường lửa trạng thái



2.4 Tường lửa trạng thái

- Giống tường lửa lọc gói tin, hoạt động ở tầng mạng, lọc gói tin đi/đến dựa trên tham số: địa chỉ nguồn, địa chỉ đích, cổng nguồn, cổng đích.
- Giống cổng mức mạch, xác định chính xác gói tin trong phiên làm việc.
- SIF hoạt động như cổng mức ứng dụng, SIF đưa gói tin lên tầng ứng dụng và kiểm tra xem nội dung dữ liệu phù hợp với các luật trong chính sách an ninh của hệ thống.



Thảo luận

Nhược điểm của tường lửa?