CHƯƠNG VII
BỨC TƯỜNG LỬA
(Firewall)

ThS. Nguyễn Cao Đạt
E-mail: dat@hcmut.edu.vn

Tham khảo

[1]. Cryptography and Network Security: chương 20

[2]. Network Security – A Beginner's Guide: module 10

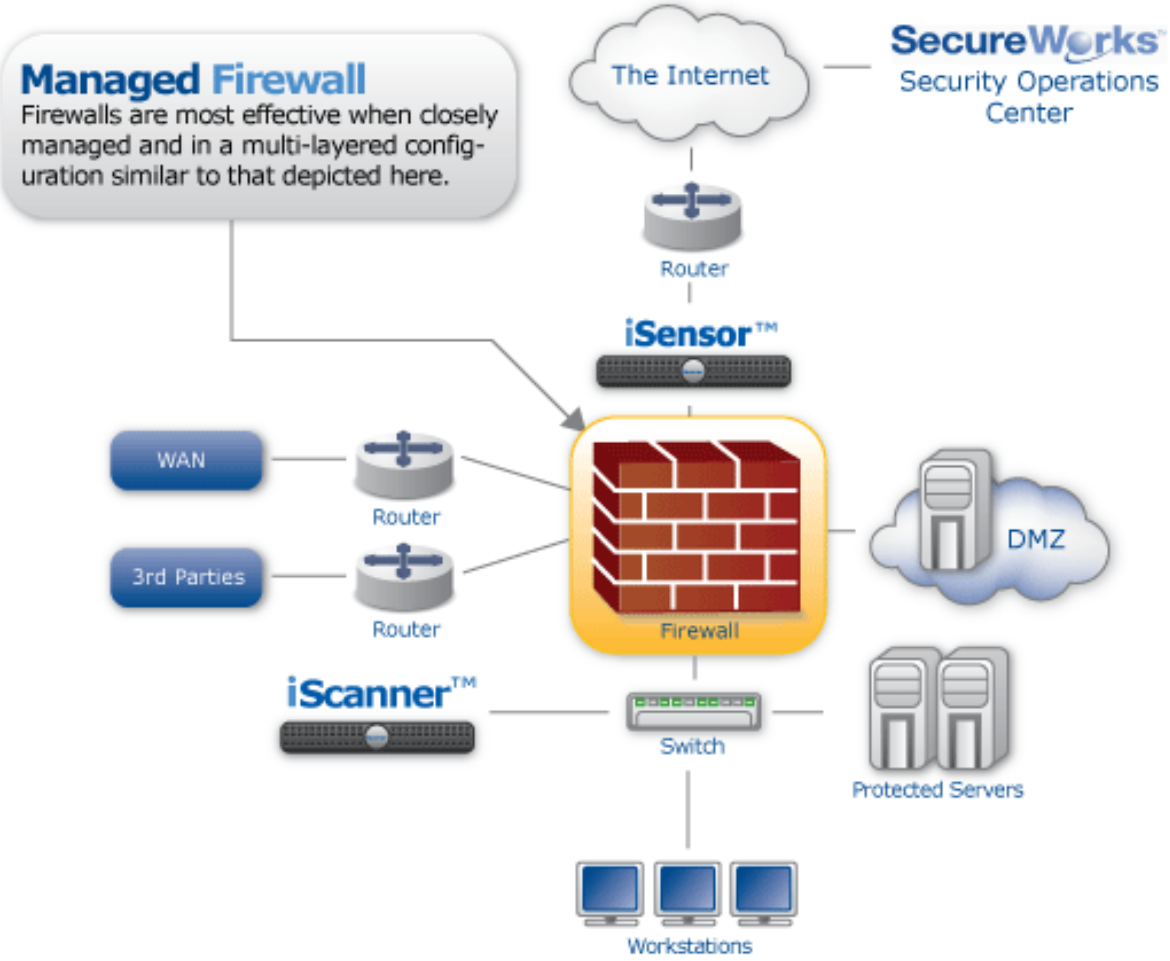
Nội dung trình bày

- Khái niệm về bức tường lửa
- Phân loại bức tường lửa
- Các cấu hình bức tường lửa
- Xây dựng tập các quy tắc
- Lựa chọn bức tường lửa để triển khai

Khái niệm về bức tường lửa

- **Một hệ thống kiểm soát truy cập mạng được thiết kế để từ chối các truy cập trái phép.**
- **Thông thường nó nằm giữa hai mạng nhằm bảo vệ một mạng từ môt mạng khác**
  - Ví dụ: Bảo vệ mạng cục bộ khi nối đến Internet
- **Tất cả thông tin liên lạc giữa hai mạng đều phải đi qua nó**
  - Điều này cho ta một điểm duy nhất để kiểm soát.
- **Lưu ý bức tường lửa khác với bộ định tuyến**
  - Tuy nhiên bộ định tuyến có thể thực hiện được một số chức năng của bức tường lửa

Khái niệm về bức tường lửa



Khái niệm về bức tường lửa

- **Mục tiêu thiết kế**
  - Tất cả thông tin liên lạc từ bên trong ra ngoài và ngược lại đều phải đi qua nó.
  - Chỉ những lưu thông mạng có quyền được phép đi qua. Các lưu thông mạng có quyền được định nghĩa bởi chính sách an ninh cục bộ.
  - Bản thân nó phải miễn dịch.

Khái niệm về bức tường lửa

- **Các kỹ thuật sử dụng**
  - Kiểm soát dịch vụ
    - Xác định các loại hình dịch vụ có thể được truy cập từ bên trong hoặc bên ngoài.
  - Kiểm soát hướng
    - Xác định hướng mà yêu cầu dịch vụ cụ thể có thể được khởi tạo và được phép lưu thông.
  - Kiểm soát người dùng
  - Kiểm soát hành vi

Khái niệm về bức tường lửa

- **Khả năng và phạm vi hoạt động**
  - Xác định một điểm chốt chặn các người dùng trái phép, các dịch vụ dễ bị tổn thương, ...
  - Cung cấp một vị trí để theo dõi, kiểm toán, báo động các sự kiện liên quan đến an ninh.
  - Một nền tảng thuận tiện cho một số chức năng Internet không liên quan đến bảo mật.
  - Phục vụ như là nền tảng cho IPSec.

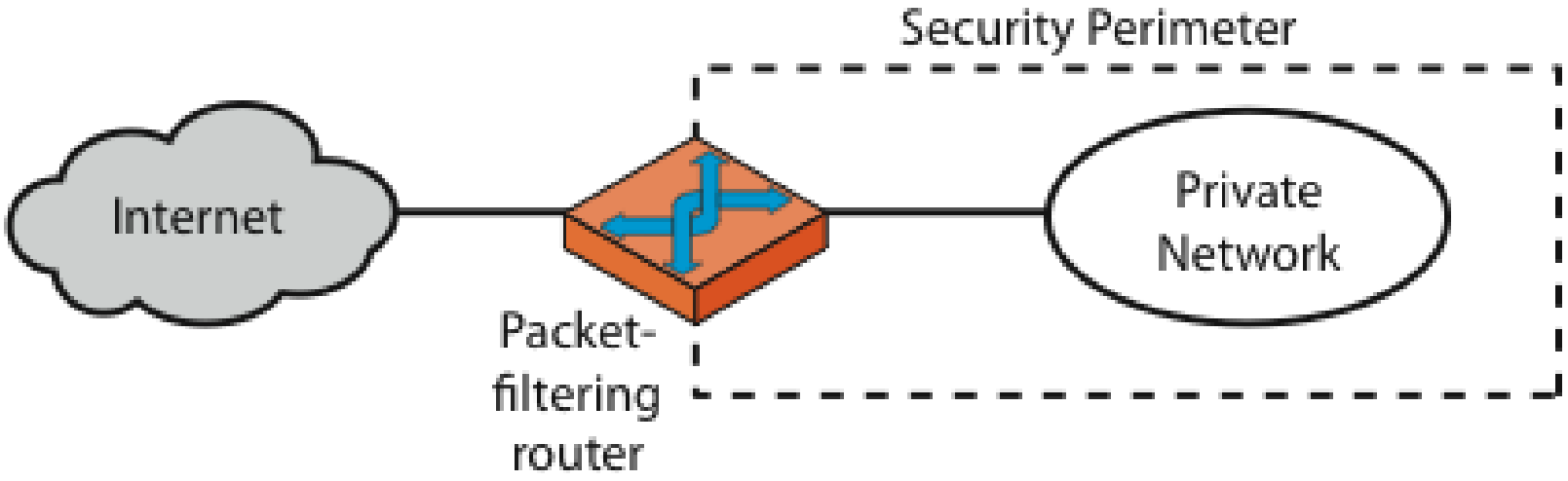
Khái niệm về bức tường lửa

- **Các hạn chế**
  - Không thể chống lại các tấn công không đi qua nó
    - Ví dụ: dial-out/dial-in, các tổ chức được tin tưởng, các dịch vụ được tin tưởng(như SSL/SSH)
  - Không thể chống lại các tấn công bên trong mạng
  - Không thể chống lại việc chuyển các tập tin hay chương trình bị nhiễm virus

Phân loại bức tường lửa

- **Bộ lọc gói (Packet-Filter)**
  - Không kiểm tra trạng thái(stateless)
  - Kiểm tra trạng thái(stateful)
- **Cổng mức ứng dụng**
  - Application level gateway
- **Cổng mức mạch**
  - Circuit level gateway

Bộ lọc gói



(a) Packet-filtering router

Bộ lọc gói

- **Áp dụng một bộ các quy tắc cho mỗi gói tin vào, ra để sau đó chuyển tiếp hoặc loại bỏ.**
- **Các quy tắc lọc dựa trên các thông tin chứa trong mỗi gói tin**
  - Địa chỉ IP nguồn, đích
  - Địa chỉ tầng vận chuyển(port) nguồn và đích
  - Các trường trong phần đầu của gói tin
  - Giao diện mạng
- **Các quy tắc**
  - Định nghĩa thông qua các tập tin cấu hình
  - Cho phép/chặn lại một cách tường minh

Ví dụ về bộ lọc gói

Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Các tấn công trên bộ lọc gói

- **Giả mạo địa chỉ IP**
  - Giả địa chỉ nguồn được tin tưởng
  - Biện pháp giải quyết: thêm các quy định trên bộ định tuyến để ngăn chặn
- **Tấn công dựa trên định tuyến từ nguồn**
  - Kẻ tấn công xét đường đi khác với mặc định
  - Biện pháp giải quyết: chặn các gói định tuyến từ nguồn
- **Tấn công phân mảnh nhỏ**
  - Chia thông tin phần đầu thành nhiều gói nhỏ
  - Biện pháp giải quyết: Loại bỏ hoặc ráp các mảnh nhỏ trước khi kiểm tra

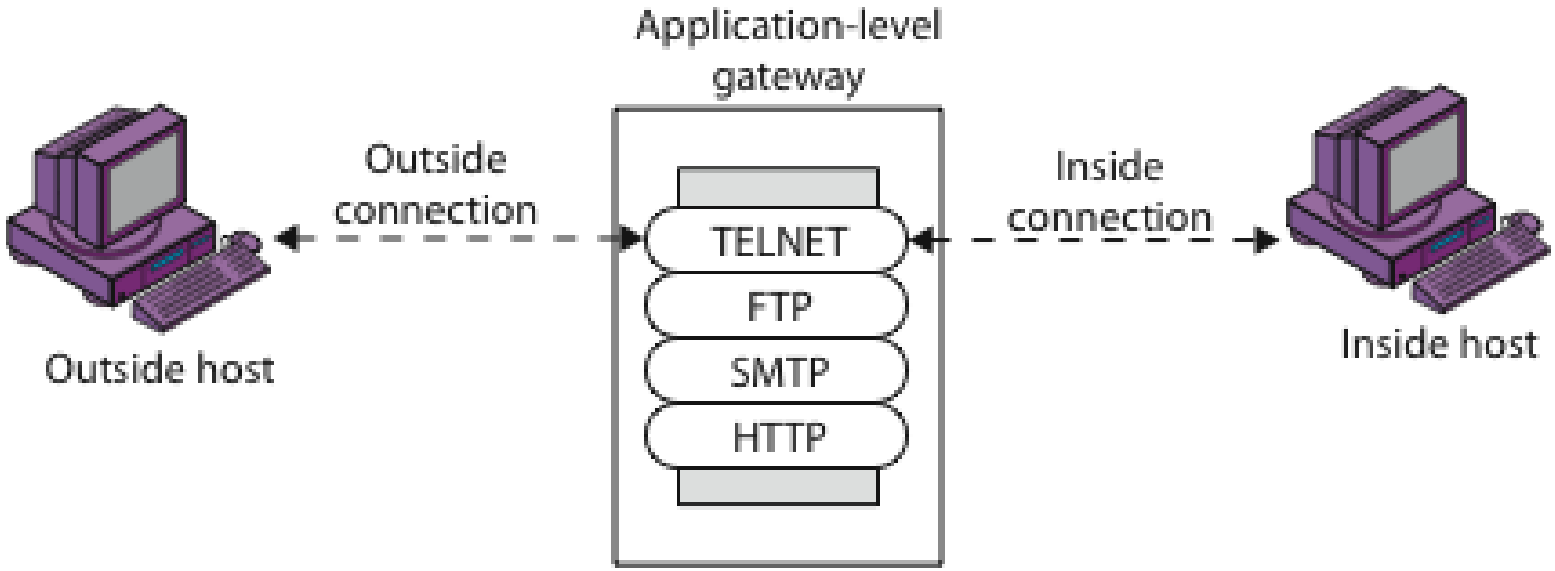
Bộ lọc gói kiểm tra trạng thái

- **Kiểm tra mỗi gói tin trong ngữ cảnh**
  - Lưu vết các kết nối giữa client-server
  - Kiểm tra mỗi gói tin thuộc vào một kết nối hợp lệ
- **Khả năng phát hiện ra các gói tin không có thật**
- **Một kết nối gắn liền với các thông tin**
  - Địa chỉ IP, port nguồn
  - Địa chỉ IP, port đích
  - Giao thức sử dụng
  - Trạng thái kết nối

Ví dụ về bảng quản lý các kết nối

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
223.212.212	1046	192.168.1.6	80	Established

Cổng mức ứng dụng

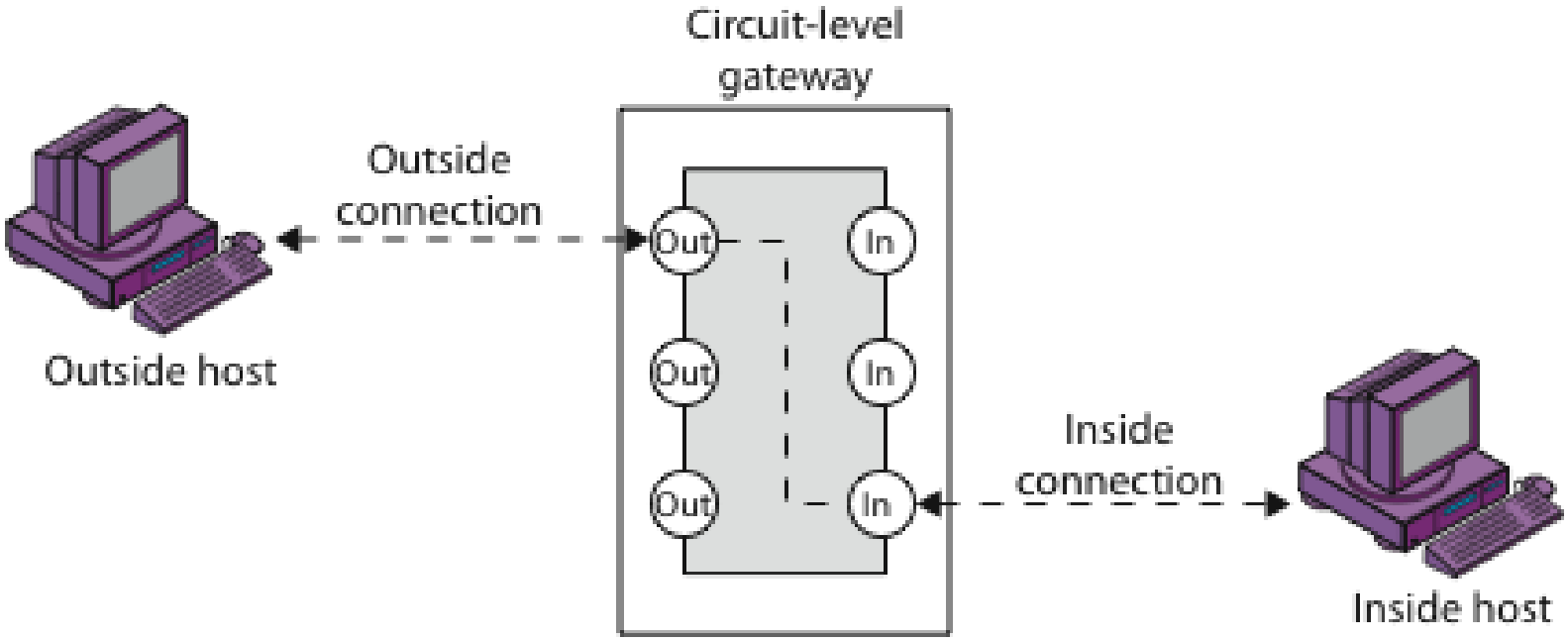


(b) Application-level gateway

Cổng mức ứng dụng

- **Đại diện cho ứng dụng cụ thể**
  - Web Proxy Server
- **Các bước xử lý**
  - Người dùng yêu cầu dịch vụ từ proxy
  - Proxy kiểm tra tính hợp lệ của yêu cầu
  - Tạo yêu cầu và lấy kết quả về cho người dùng
  - Có thể ghi lại/kiểm toán lưu thông mạng ở mức ứng dụng
- **Các bất lợi khi dùng cổng mức ứng dụng**
  - Cần có proxy riêng biệt cho mỗi dịch vụ
  - Chi phí xử lý bổ sung trên mỗi kết nối. Có vấn đề trên một số dịch vụ.

Cổng mức mạch

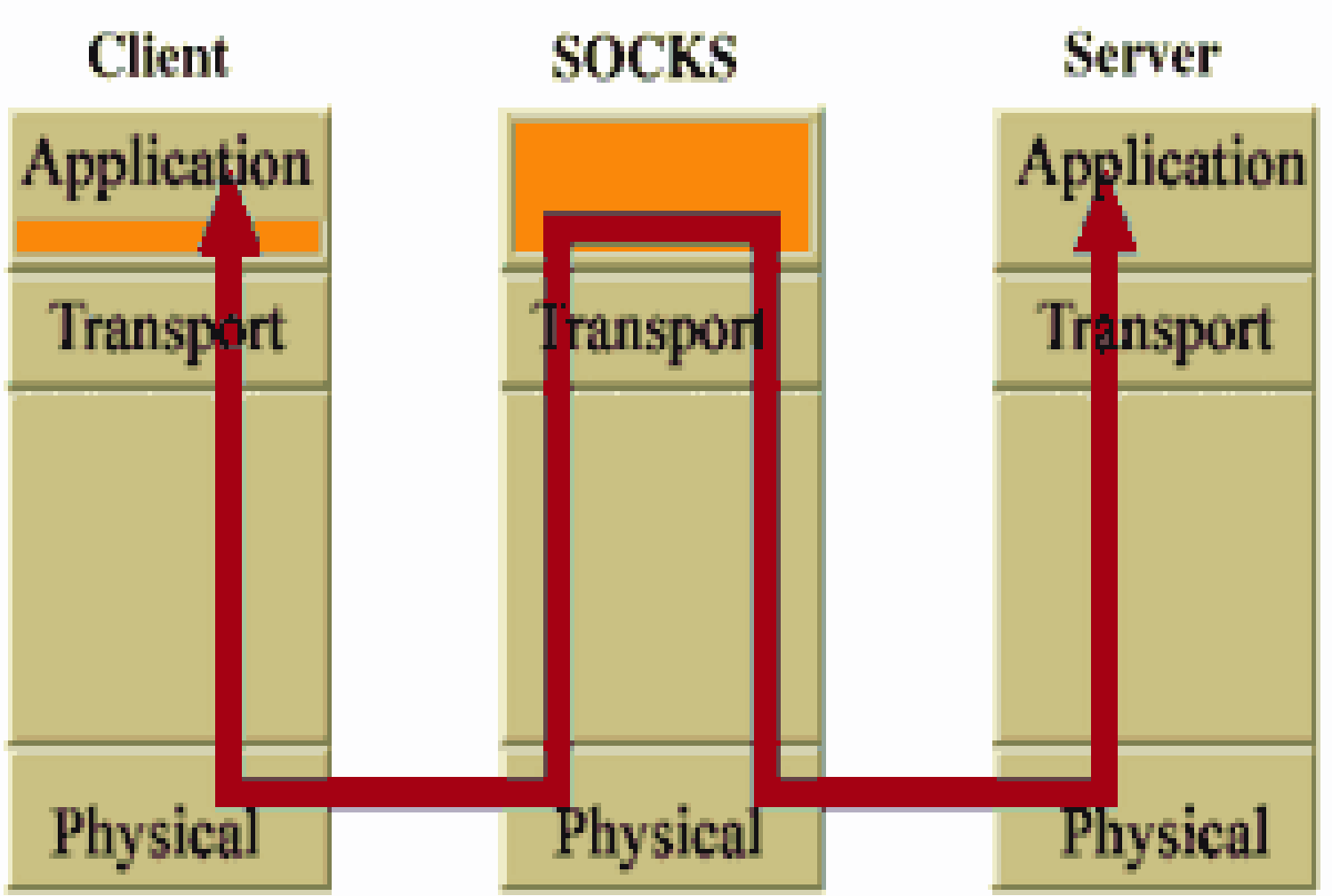


(c) Circuit-level gateway

Cổng mức mạch

- **Tạo hai kết nối TCP**
  - Một kết nối giữa nó và bên trong
  - Một kết nối giữa nó và bên ngoài
- **Giới hạn các kết nối được cho phép**
- **Thường thực hiện chuyển tiếp mà không kiểm tra nội dung của gói tin**
- Thường được dùng khi tin tưởng các người dùng cục bộ, cho phép họ tạo các kết nối ra ngoài một cách tổng quát

Cổng mức mạch



Bastion Host

- Thông thường bức tường lửa được biết đến như "bastion host"
- Một máy chủ rút gọn
  - Không có các dịch vụ không cần thiết
  - Không có ứng dụng không cần thiết
  - Không có thiết bị không cần thiết

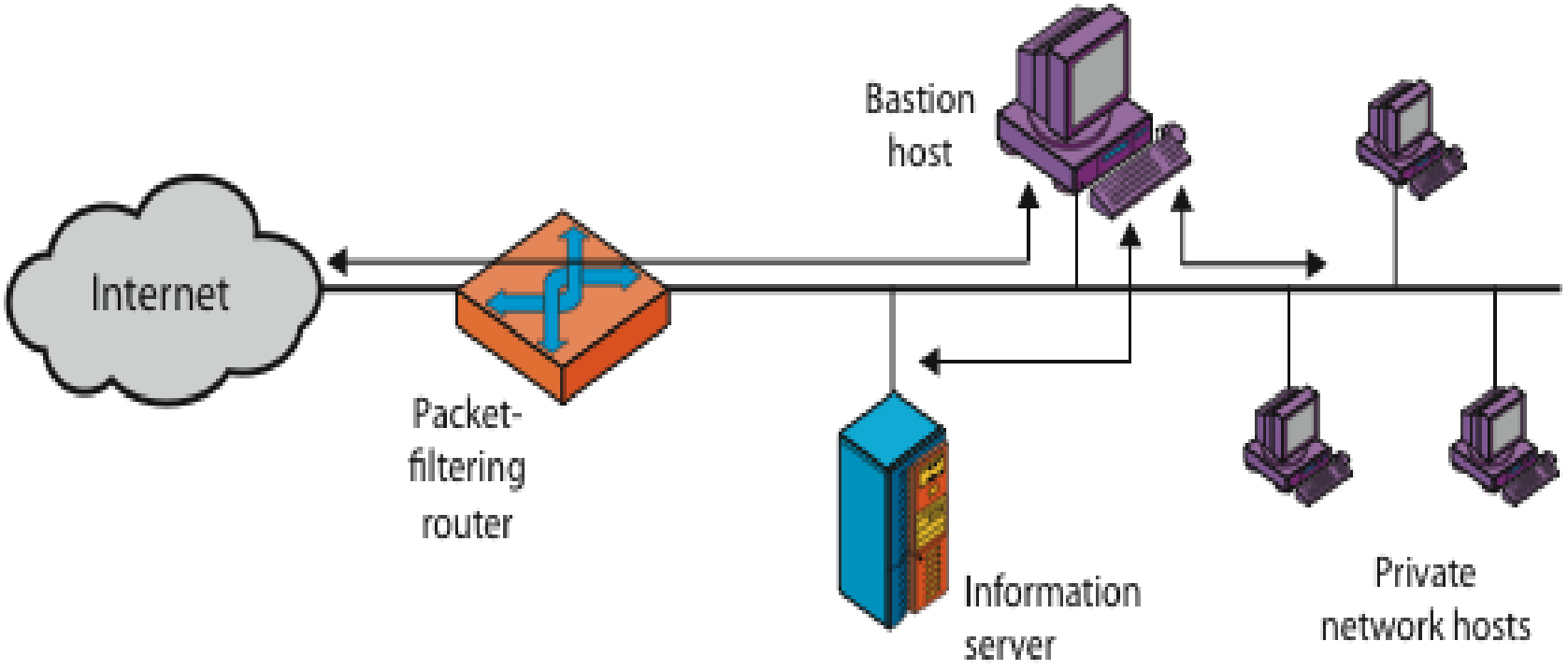
Bastion Host

- **Các đặc điểm chính**
  - Thực thi một phiên bản hệ điều hành an toàn
  - Chỉ cài đặt một số dịch vụ thiết yếu
  - Yêu cầu xác thực bổ sung
  - Hỗ trợ chỉ một tập con các lệnh ở mức ứng dụng
  - Duy trì thông tin kiểm toán chi tiết
  - Có hai hay nhiều giao tiếp mạng

Các cấu hình bức tường lửa

- **Screened Host**
  - Single Homed Bastion Host
  - Dual Homed Bastion Host
- **Screened Subnet**

Single-homed Bastion

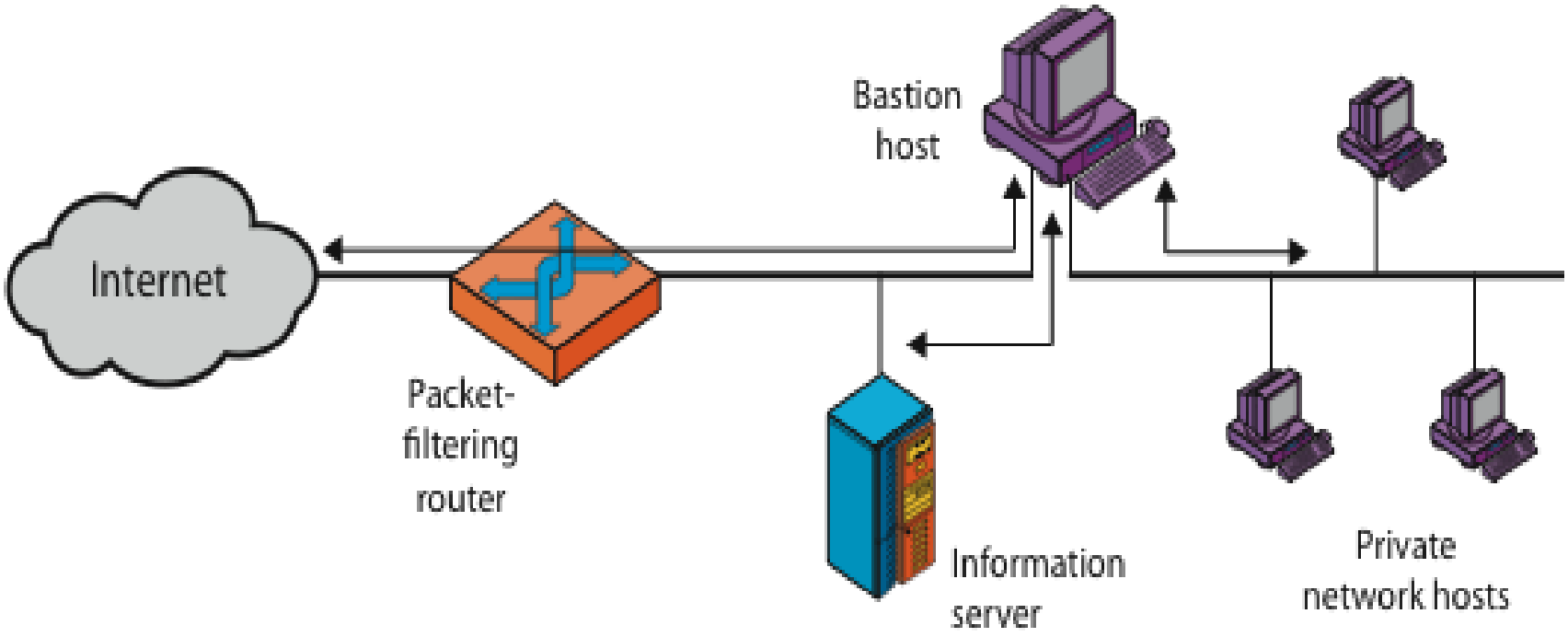


(a) Screened host firewall system (single-homed bastion host)

Single-homed Bastion

- **Bao gồm hai hệ thống**
  - Một bộ lọc gói
  - Một bastion host
  - An toàn hơn
- **Kiểm soát trên bộ lọc gói**
  - Các lưu thông mạng từ Internet đi vào chỉ được cho phép nếu địa chỉ đích đến là bastion host.
  - Các lưu thông mạng từ mạng bên trong đi ra chỉ có các gói từ bastion host là cho phép.
- **Bastion host cung cấp các chức năng xác thực và đại diện cung cấp dịch vụ(proxy)**

Dual-homed Bastion

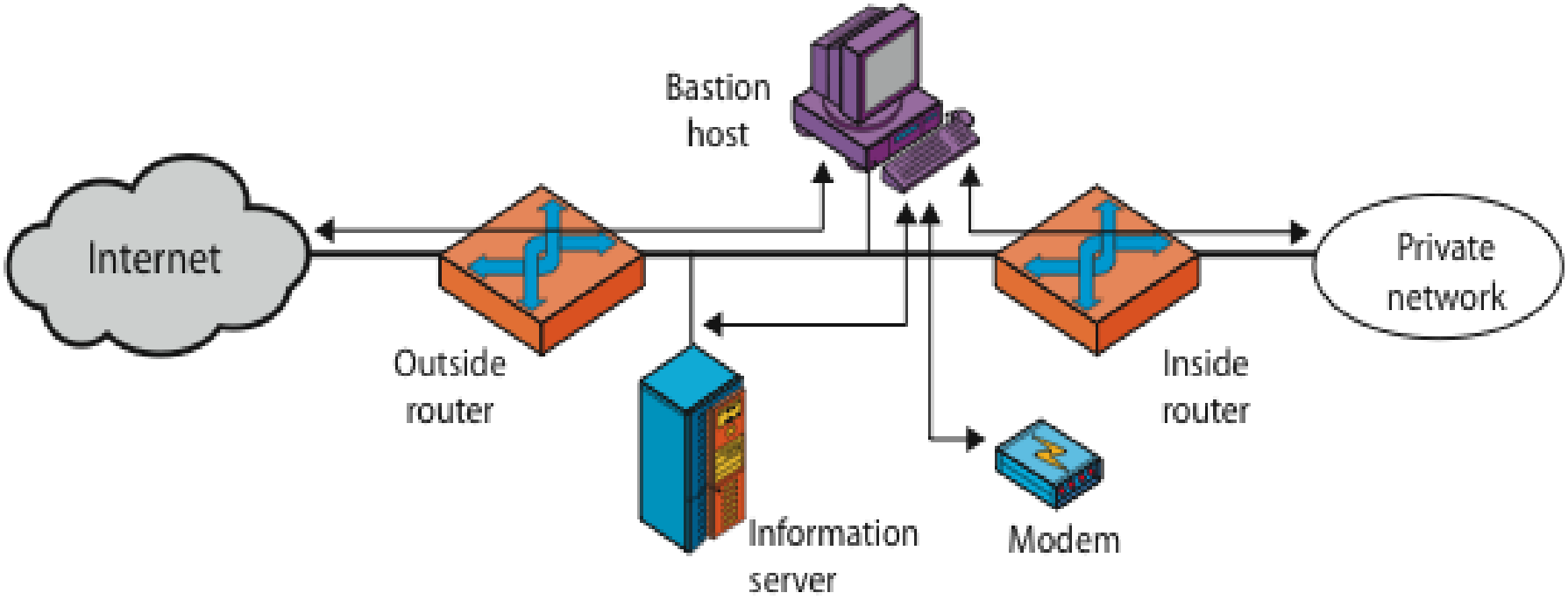


(b) Screened host firewall system (dual-homed bastion host)

Dual-homed Bastion

- **Bastion host có hai giao tiếp mạng**
  - Chia thành mạng bên trong thành 2 mạng con
  - Tăng cường tính an toàn
- **Khi bộ lọc gói bị thỏa hiệp**
  - Lưu thông mạng từ Internet không thể trực tiếp đi vào mạng riêng bên trong

Screened Subnet



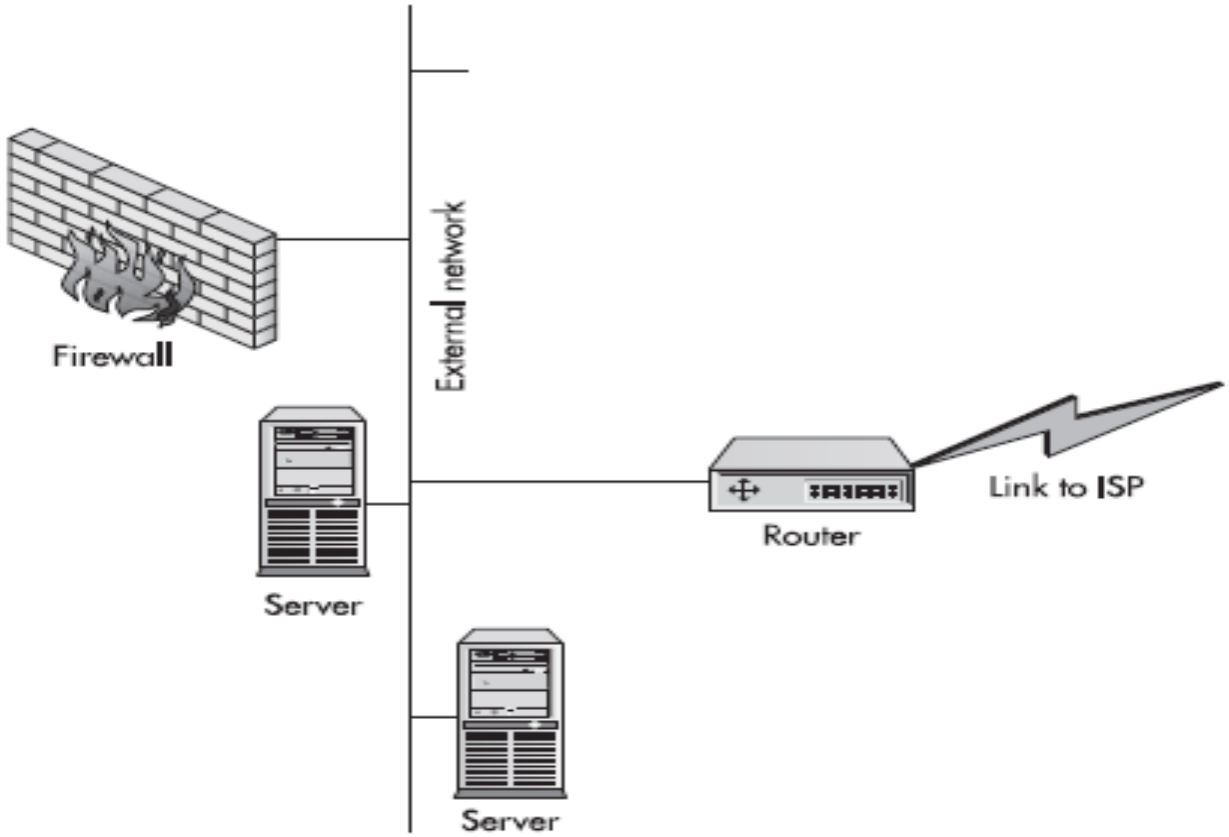
(c) Screened-subnet firewall system

Screened Subnet

- **Bao gồm ba hệ thống**
  - Hai bộ lọc gói, một bastion host.
  - Tạo ra một mạng con được cô lập bao gồm các máy chủ, bastion host.
- **Các lợi thế**
  - Có ba cấp độ bảo vệ để ngăn chặn những kẻ xâm nhập.
  - Bộ lọc gói bên ngoài chỉ quảng bá mạng con được cô lập nên mạng nội bộ bên trong xem như vô hình với Internet.
  - Tương tự bộ lọc gói bên trong quảng bá mạng con được cô lập do đó các máy tính của mạng nội bộ bên trong không có thể tạo kết nối trực tiếp với Internet.

Xây dựng tập quy tắc

- **Kiến trúc 1 – Cho phép bên trong truy cập đến một số hệ thống trên Internet**



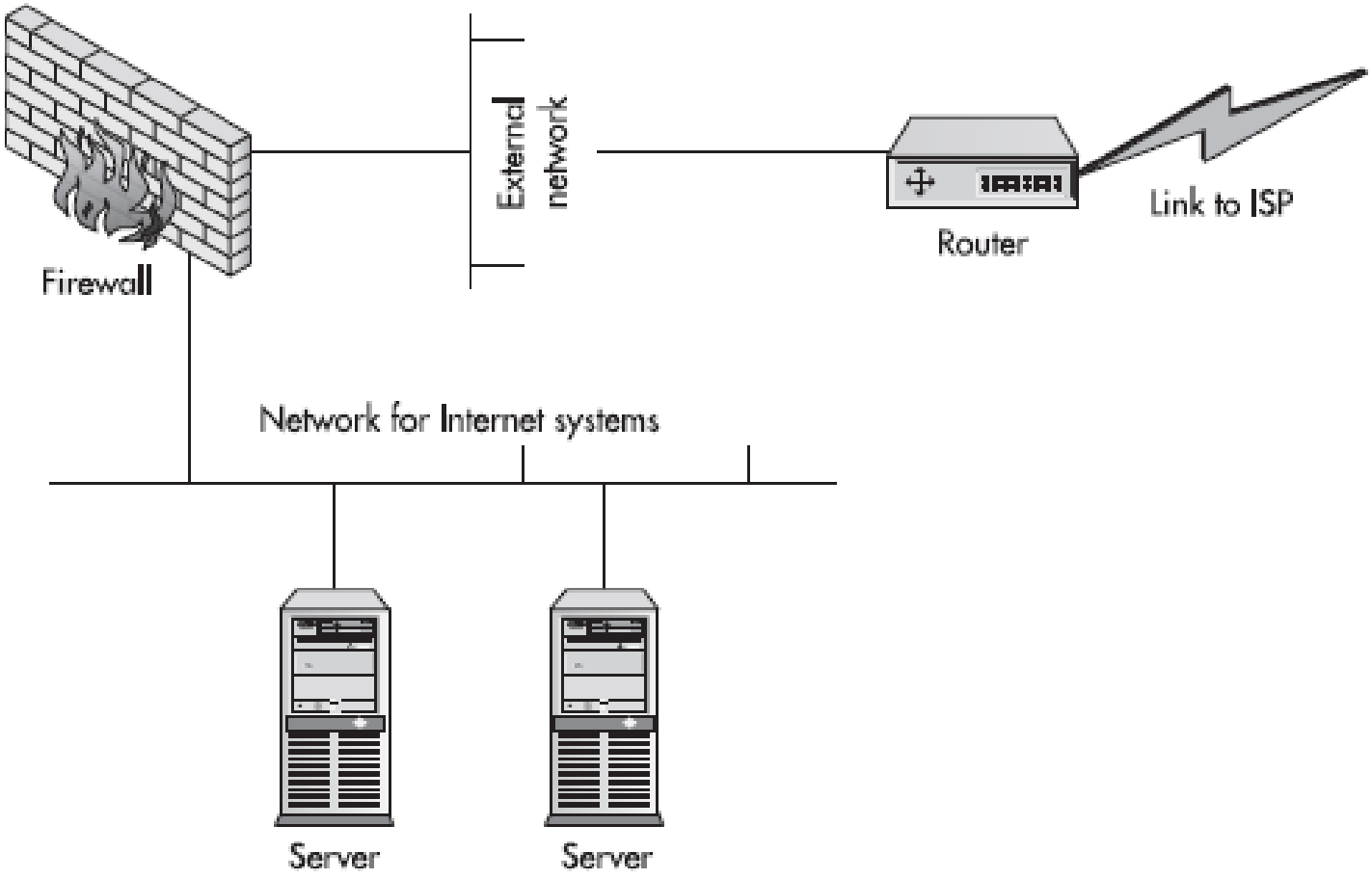
Xây dựng tập quy tắc

- **Tập quy tắc đề xuất cho kiến trúc 1**

STT	Địa chỉ IP nguồn	Địa chỉ IP đích	Dịch vụ	Hành động
1	Mail Server nội bộ	Mail Server	SMTP	Chấp nhận
2	đ/c mạng nội bộ	Bất kỳ	HTTP, HTTPS, FTP, SSH	Chấp nhận
3	DNS Server nội bộ	Bất kỳ	DNS	Chấp nhận
4	Bất kỳ	Bất kỳ	Bất kỳ	Loại bỏ

Xây dựng tập quy tắc

- **Kiến trúc 2 – Cung cấp dịch vụ Internet**



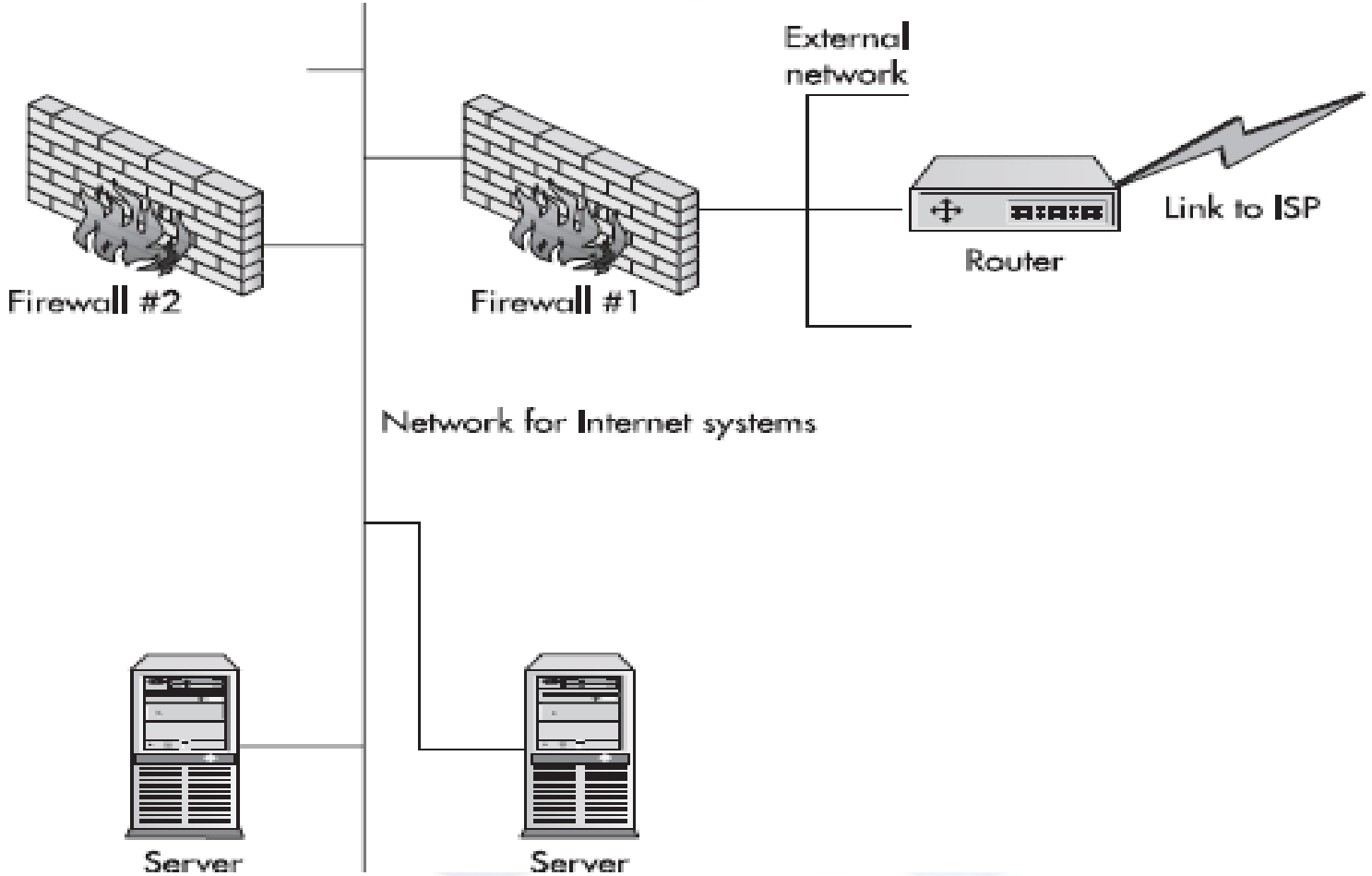
Xây dựng tập quy tắc

- **Tập quy tắc đề xuất cho kiến trúc 2**

STT	Địa chỉ IP nguồn	Địa chỉ IP đích	Dịch vụ	Hành động
1	Bất kỳ	Web Server	HTTP, HTTPS	Chấp nhận
2	Bất kỳ	Mail Server	SMTP	Chấp nhận
3	Mail Server	Bất kỳ	SMTP	Chấp nhận
4	đ/c mạng nội bộ	Bất kỳ	HTTP, HTTPS, FTP, SSH	Chấp nhận
5	DNS Server nội bộ	Bất kỳ	DNS	Chấp nhận
6	Bất kỳ	Bất kỳ	Bất kỳ	Loại bỏ

Xây dựng tập quy tắc

- **Kiến trúc 3 – Hai bức tường lửa**



Xây dựng tập quy tắc

- **Tập quy tắc đề xuất cho kiến trúc 3**
  - Trên bức tường lửa 1

STT	Địa chỉ IP nguồn	Địa chỉ IP đích	Dịch vụ	Hành động
1	Bất kỳ	Web Server	HTTP, HTTPS	Chấp nhận
2	Bất kỳ	Mail Server	SMTP	Chấp nhận
3	Mail Server	Bất kỳ	SMTP	Chấp nhận
2	đ/c mạng nội bộ	Bất kỳ	HTTP, HTTPS, FTP, SSH	Chấp nhận
3	DNS Server nội bộ	Bất kỳ	DNS	Chấp nhận
4	Bất kỳ	Bất kỳ	Bất kỳ	Loại bỏ

Xây dựng tập quy tắc

- **Tập quy tắc đề xuất cho kiến trúc 3**
  - Trên bức tường lửa 2

STT	Địa chỉ IP nguồn	Địa chỉ IP đích	Dịch vụ	Hành động
1	Mail Server nội bộ	Mail Server	SMTP	Chấp nhận
2	đ/c mạng nội bộ	Bất kỳ	HTTP, HTTPS, FTP, SSH	Chấp nhận
3	DNS Server nội bộ	Bất kỳ	DNS	Chấp nhận
4	Bất kỳ	Bất kỳ	Bất kỳ	Loại bỏ

Lựa chọn Firewall để triển khai

- **Các tính năng cần quan tâm**
  - Dùng cho cá nhân hay cho một tổ chức
  - Bộ lọc gói có kiểm tra trạng thái
  - Quản lý các mối đe dọa một cách thống nhất(UTM - Unified Threat Management) như lọc Web, bảo vệ VoIP, quét Virus, quét Spam, kiểm soát ứng dụng, ..
  - Dễ sử dụng
  - Hiệu suất cao
  - Có khả năng chịu lỗi
  - Cài đặt và triển khai dễ dàng

Lựa chọn Firewall để triển khai

- **Các Firewall cá nhân**
  - ZoneAlarm: http://www.zonelabs.com/
  - Comodo Firewall: http://personalfirewall.comodo.com/
  - Tiny Personal Firewall: http://www.tinysoftware.com/
  - Norton Personal Firewall: http://www.symantec.com/
- **Các Firewall dành cho các tổ chức**
  - Checkpoint: http://www.checkpoint.com/
  - Juniper: http://www.juniper.net/
  - Fortinet: http://www.fortinet.com/
  - Watchguard: http://www.watchguard.com/
  - SonicWALL: http://www.sonicwall.com/

Tóm tắt

- Bức tường lửa tạo thành một rào cản mà các truy cập ở các hướng muốn thành công phải vượt qua. Các quy tắc hiện thực chính sách an ninh được cấu hình trên bức tường lửa nhằm kiểm soát và chỉ cho phép các truy cập có thẩm quyền được đi qua.
- Một bức tường lửa có thể được thiết kế để hoạt động như một lọc gói tin IP hoặc có thể hoạt động ở một giao thức cao hơn.
- Khi lựa chọn để triển khai một bức tường lửa cần lưu ý đến một số tính năng.
- Thứ tự các quy tắc trong mỗi bộ định tuyến rất quan trọng.