

Trường Đại Học Công Nghệ Thông Tin
Khoa Mạng Máy Tính và Truyền Thông

AN TOÀN MẠNG MÁY TÍNH

ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan
2. Các phần mềm gây hại – Trojan
3. Các phần mềm gây hại – Virus
4. Các giải thuật mã hoá dữ liệu
5. Mã hoá khoá công khai và quản lý khoá
6. Chứng thực dữ liệu
7. Một số giao thức bảo mật mạng
8. Bảo mật mạng không dây
9. Bảo mật mạng ngoại vi
10. Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

BÀI 9

BẢO MẬT MẠNG NGOẠI VI



NỘI DUNG BÀI HỌC

1. Tổng quan
2. Bộ lọc gói tin (Packet Filters)
3. Cổng mạch (Circuit Gateways)
4. Cổng ứng dụng (Application Gateways)
5. Bastion Hosts
6. Cấu hình tường lửa
7. Chuyển dịch địa chỉ mạng (NAT)
8. TMG – Threat Management Gateway
9. Bài tập

1. Tổng quan

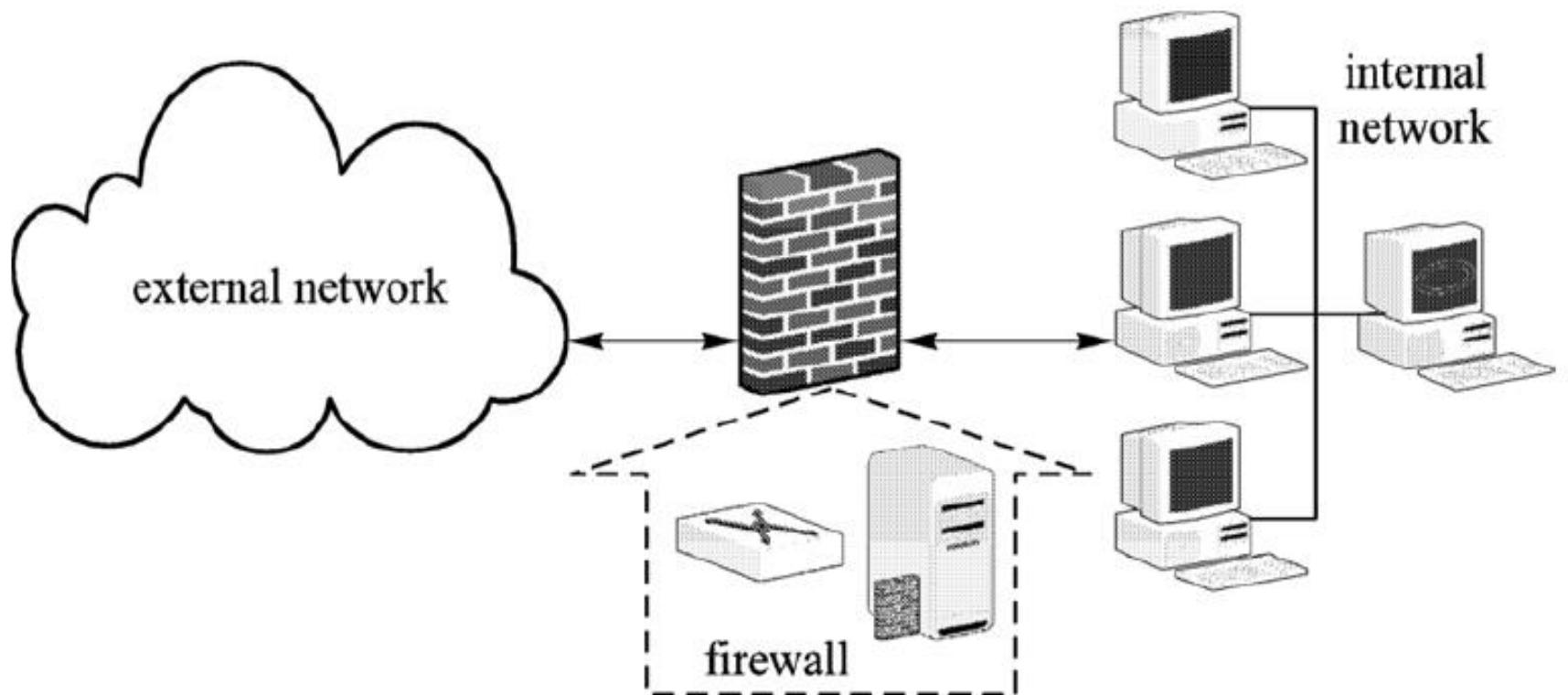
- Các thuật toán mã hoá không hiệu quả khi ngăn chặn các gói tin độc hại đi vào mạng cục bộ.
- Các giải thuật chứng thực có thể được sử dụng để xác định các gói tin đến từ các user tin cậy và giúp ngăn chặn các gói tin độc hại đi vào mạng.
- Tuy nhiên, các máy tính trong mạng đa số đều không có đủ tài nguyên, phương tiện... để thực hiện các giải thuật chứng thực trong mọi tình huống.

→ *Kỹ thuật tường lửa (Firewall)*

1. Tổng quan

- Tường lửa được phát triển trong những năm 1980, là công cụ quan trọng của các tổ chức, công ty, cơ quan nhà nước, cá nhân... dùng để hạn chế việc truy cập mạng nhằm bảo mật cho mạng nội bộ.
- Tường lửa được sử dụng như một hàng rào ngăn cách giữa vùng không đáng tin cậy là mạng Internet (external network) và vùng có độ tin cậy cao là mạng nội bộ (internal network), ngăn chặn hoặc cho phép các gói tin đi qua giữa hai mạng này dựa trên nguyên tắc quyền tối thiểu.

1. Tổng quan

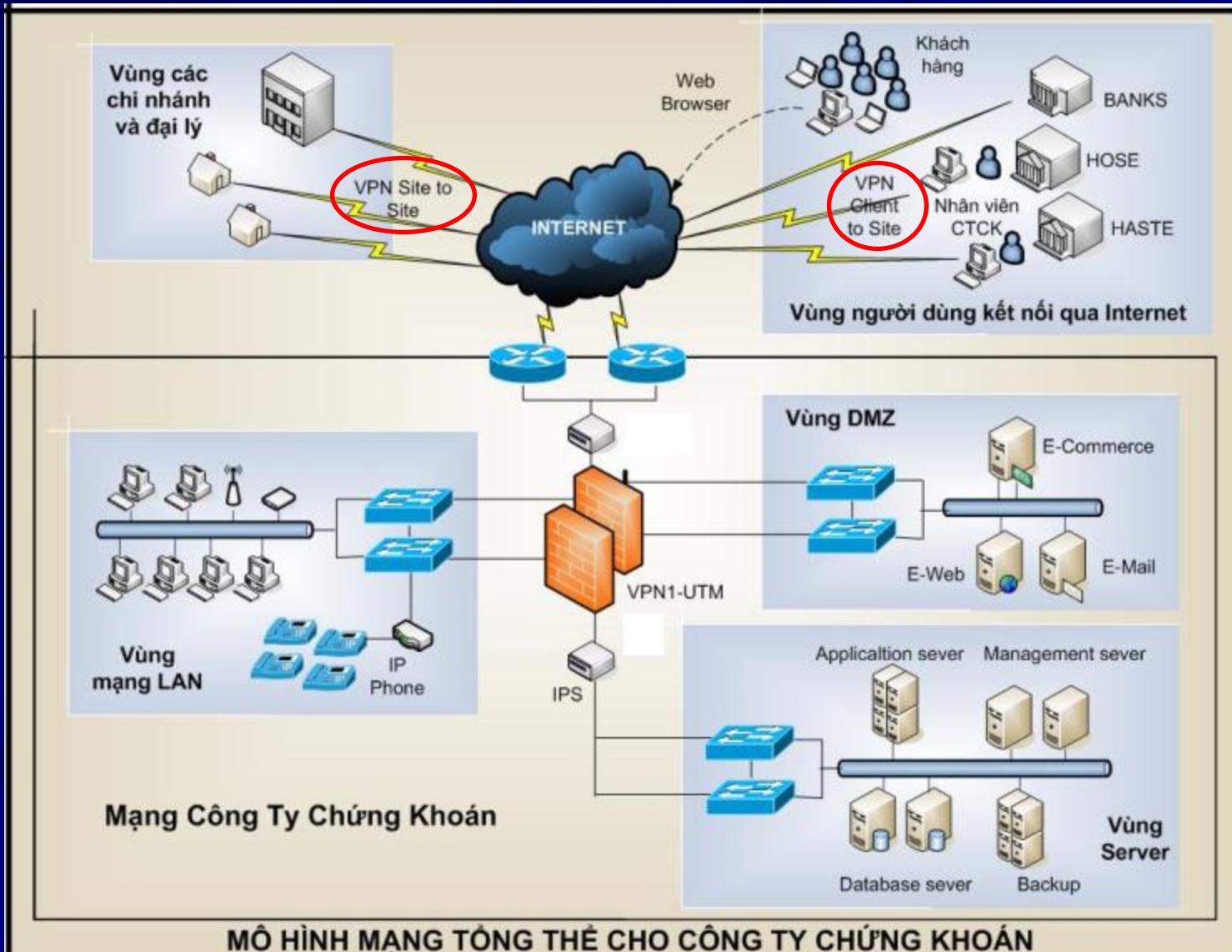


Schematic of a firewall

1. Tổng quan

- Tường lửa có thể là một thiết bị phần cứng, một gói phần mềm hoặc là sự kết hợp của cả hai.
- Tường lửa có thể được nhúng vào các thiết bị mạng phổ biến như router, switch, modem, wireless access point.
- Tường lửa cứng (phần cứng) nhanh nhưng khó cập nhật.
- Tường lửa mềm (phần mềm) linh hoạt hơn vì dễ dàng cập nhật.

1. Tổng quan



1. Tổng quan

■ Một số tường lửa cứng (phần cứng) thông dụng:

1. Cisco Router



2. FortiNet



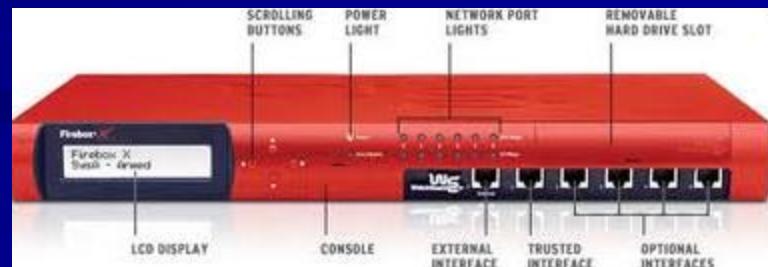
3. CheckPoint Safe@Office



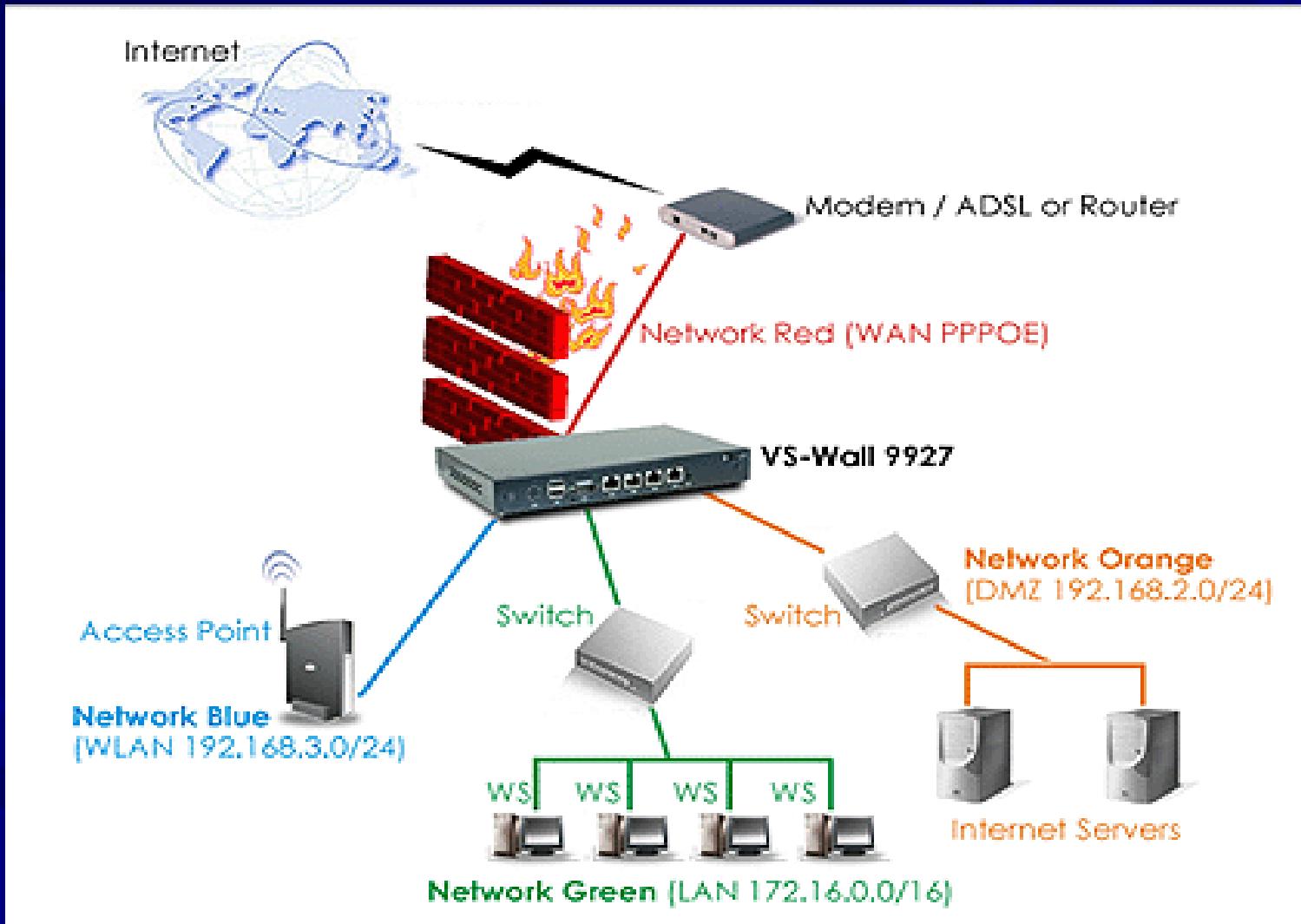
4. Sonicwall PRO



5. WatchGuard Firebox



1. Tổng quan



1. Tổng quan

- Một số tường lửa mềm (phần mềm) thông dụng:
 1. Comodo Firewall
 2. ESET Smart Security
 3. ZoneAlarm
 4. Outpost Firewall Pro
 5. F-Secure Internet Security



1. Tổng quan

Giao diện ISA Management Console

The screenshot shows the Microsoft Internet Security and Acceleration Server 2006 Beta Management Console. The left sidebar navigation includes 'Monitoring', 'Firewall Policy' (selected), 'Virtual Private Networks (VPN)', 'Configuration' (with 'Networks', 'Cache', 'Add-ins', 'General'), and 'File' menu items. The main area displays the 'Firewall Policy' table:

| Order | Name | Action | Protocols | From / Listener | To |
|-------|---------------|--------|--------------------------------------|---------------------------------------|---------------------------------------|
| 1 | http | Deny | HTTP | Intern | Extern |
| 2 | vpn | Allow | PPTP PPTP-Server | Extern Lokaler Host | Lokaler Host |
| 3 | intern | Allow | All Outbound ... | Intern | Lokaler Host |
| 4 | isa | Allow | RPC (alle Sch... RPC-Server (...) | Extern Lokaler Host | Lokaler Host |
| 5 | proxy | Allow | All Outbound ... | Intern | Extern |
| 6 | ales | Allow | All Outbound ... | Intern Lokaler Host | Intern Lokaler Host |
| 7 | vpn2 | Allow | All Outbound ... | Intern Lokaler Host VPN-Clients | Intern Lokaler Host VPN-Clients |
| Last | Standardregel | Deny | All Traffic | Alle Netzwerk... | Alle Netzwerk |

The right pane contains a 'Toolbox' with 'Protocols', 'Users', 'Content Types', 'Schedules', and 'Network Objects' sections, and a 'Task Pane' with 'New', 'Edit...', and 'Delete' buttons.

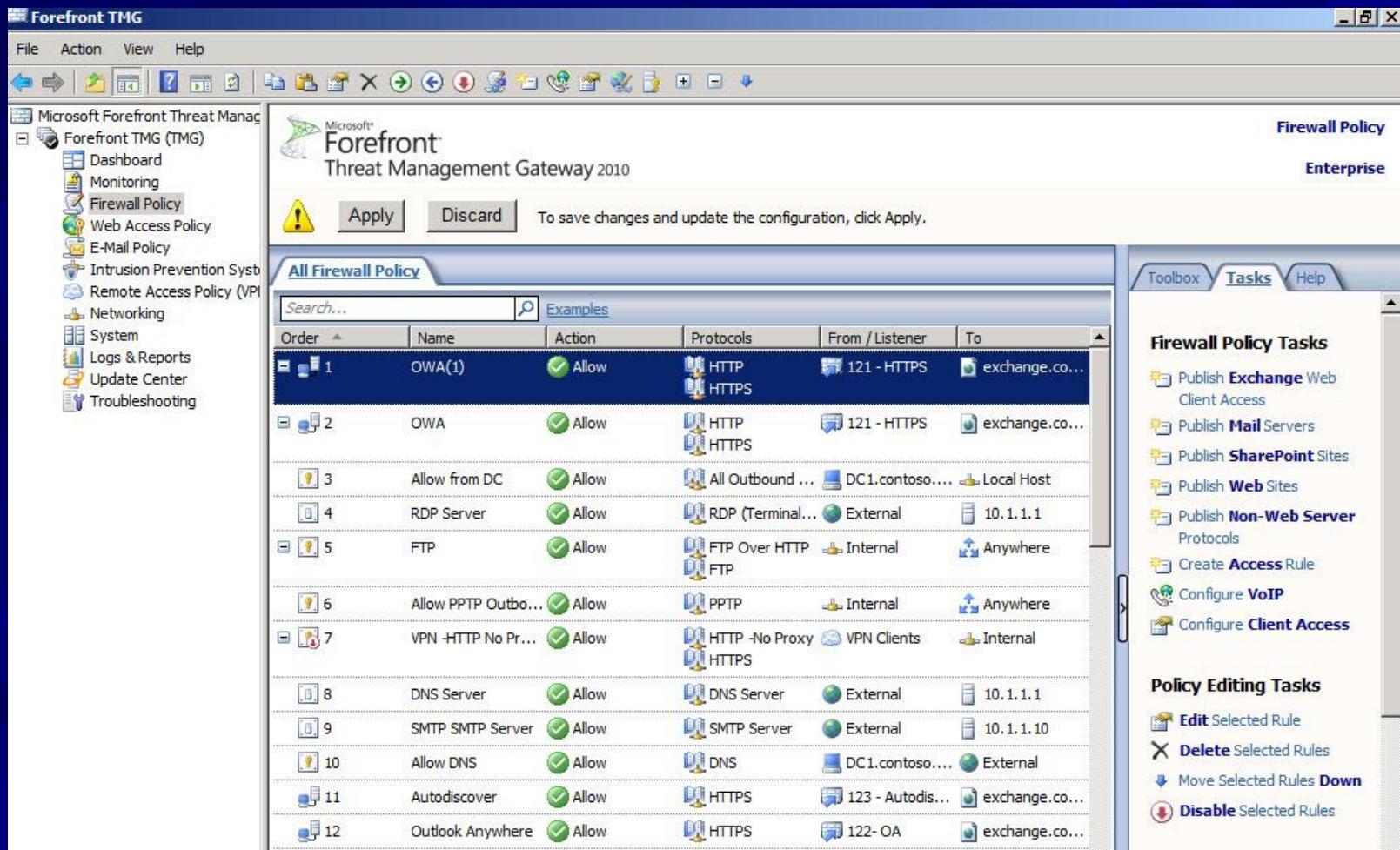
Duyệt các chức năng chính như Server name, Monitoring, Firewall Policy, Cache...

Hiển thị các chi tiết thành phần chính để chọn lựa như System Policy, Access Rule...

Task Pane:
chứa các dịch vụ đặc biệt như Publishing Server, Enable VPN Server...

1. Tổng quan

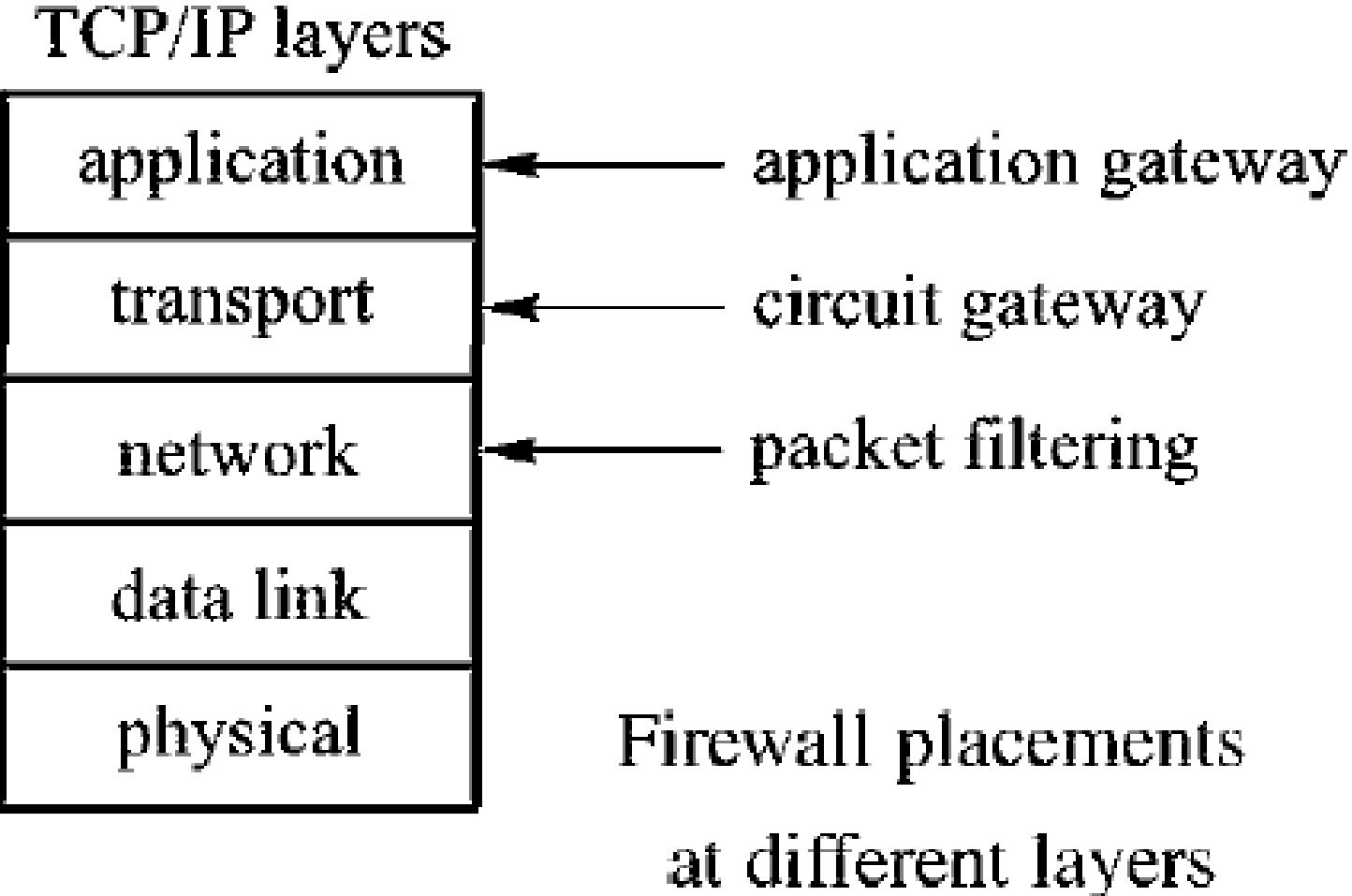
Giao diện Microsoft Forefront TMG 2010



1. Tổng quan

- Dựa trên các phương thức đặc trưng riêng, tường lửa có thể được phân thành các loại:
 - packet filter: kiểm tra cả IP header lẫn TCP header.
 - circuit gateway
 - application gateway
 - dynamic packet filter: là tường lửa lai, kết hợp cả hai loại packet filter và circuit gateway vào trong một hệ thống tường lửa.

1. Tổng quan



2. Bộ lọc gói tin (Packet Filter)

Khái niệm chung

- Là kỹ thuật tường lửa cơ bản.
- Kiểm tra các gói tin từ bên ngoài đi vào mạng nội bộ và từ mạng nội bộ đi ra bên ngoài.
- Chỉ kiểm tra IP header và TCP header, không kiểm tra phần payload sinh ra từ lớp ứng dụng.
- Sử dụng một tập các quy tắc để quyết định xem gói tin nào được cho phép hoặc bị từ chối đi vào (ra).
- Gồm hai loại:
 - *stateless filtering* (bộ lọc phi trạng thái)
 - *stateful filtering* (bộ lọc có trạng thái)

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc phi trạng thái

- Là kỹ thuật tương lừa đơn giản nhất và được sử dụng rộng rãi nhất.
xử lý mỗi request là độc lập
- Xử lý mỗi gói tin như một đối tượng độc lập.
- Kiểm tra một gói tin khi nó đến, ra quyết định phù hợp và không lưu lại bất kỳ thông tin nào về gói tin này.
- Cách xử lý của bộ lọc này tương tự như việc phân loại chuyển phát thư của ngành bưu điện. Người ta sắp xếp và kiểm tra mỗi bao thư để chắc chắn địa chỉ đích là hợp lệ.

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc phi trạng thái

- Tổng quát, bộ lọc phi trạng thái thường kiểm tra
 - Địa chỉ IP nguồn và đích trong IP header theo một tập quy tắc đã được xác định trước.
 - Port nguồn và port đích trong một TCP header hoặc UDP header.
 - Tập quy tắc thường được gọi là một Access control list (ACL).
- Vì lớp mạng có nhiệm vụ kiểm tra IP header để có thể phân phối các gói tin nên việc hiện thực bộ lọc gói tại lớp mạng không đòi hỏi phải tính toán nhiều.

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc phi trạng thái

Sample ACL rules for ingress filtering, where “int” represents “internal”, “ext” represents “external”, and “addr” represents “address”

| int addr | int port | ext addr | ext port | action | comment |
|--------------|----------|----------|----------|--------|------------------------------------|
| * | * | a.b.c.d | * | block | block packets from this IP address |
| 192.63.8.254 | 110 | * | * | allow | open internal POP3 port |

2 loại ACL, đặc điểm và nguyên tắc cơ bản của chúng

Sample ACL rules for egress filtering

| int addr | int port | ext addr | ext port | action | comment |
|----------|----------|----------|----------|--------|-------------------------------------|
| * | * | a.b.c.d | * | block | block packets to this IP address |
| * | * | * | 25 | allow | allow packets to external SMTP port |
| * | * | * | > 1023 | allow | allow packets to non-standard port |

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc phi trạng thái

Standard Access-list

```
Router(config)#access-list n {permit | deny} source.IP wildcard-mask  
Router(config-if)#ip access-group n {in | out}
```

thiết lập cho ACL là có deny all
vị trí đặt
lệnh của 2 ACL
thực hiện lệnh từ trên xuống
sắp xếp từ chi tiết đến tổng quát

Extended Access-list

```
Router(config)#access-list n {permit | deny} protocol(IP,TCP,UDP,...) source.IP  
wildcard-mask source.port desport des.IP wildcard-mask source.port des.port  
Router(config-if)#ip access-group n {in | out} Router(config-if)#ip access-group n {in |  
out}
```

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc phi trạng thái

- **Ưu điểm:** dễ thực hiện, vì chỉ kiểm tra các IP header và TCP header.
- **Nhược điểm:**
 - Không ngăn chặn được các gói tin độc hại khai thác sơ hở của các phần mềm ở tầng ứng dụng.
 - Do mỗi gói tin phải được kiểm tra đối với toàn bộ ACL, có thể gây nên một nút cổ chai trên một mạng tốc độ cao, dẫn đến thất thoát gói tin và giảm tốc độ truyền ngoài ý muốn.

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc có trạng thái

- Bộ lọc có trạng thái còn được gọi là bộ lọc trạng thái kết nối (connection-state filtering), **giữ lại thông tin về kết nối giữa một host nội bộ và một host bên ngoài.**
- Một trạng thái kết nối chỉ ra đó là kết nối TCP hay UDP và kết nối này có được thiết lập hay không.
- Trạng thái kết nối được lưu trong một bảng trạng thái (state table).

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc có trạng thái

- Khi một gói tin đến (vào hay ra), bộ lọc sẽ kiểm tra xem gói tin này đã có trong bảng trạng thái hay chưa.
 - Nếu có, tường lửa sẽ cho gói tin đi qua và lưu lại thông tin (TCP sequence number...) cho lần sau.
 - Nếu gói tin này là gói SYN, tường lửa sẽ tạo một entry mới trong bảng trạng thái.
 - Nếu gói tin không thuộc về một kết nối đã có và nó không phải là một gói SYN, tường lửa sẽ huỷ nó.

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc có trạng thái

- Số port là một số dương dùng để nhận diện một chương trình riêng biệt. Bất kỳ một port nào được mở bởi một host nội bộ ngầm định sẽ có số port nhỏ hơn 1024.
- Số port nhỏ hơn 1024 là port chuẩn.
- Ngầm định, host bên ngoài sẽ sử dụng số port giữa 1024 và 65535 để thực thi một kết nối với host nội bộ.

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc có trạng thái

Example of connection state table

| client addr | client port | server addr | server port | connection state | protocol |
|---------------|-------------|--------------|-------------|------------------|----------|
| 219.22.101.32 | 1030 | 129.63.24.84 | 25 | established | TCP |
| 219.22.101.54 | 1034 | 129.63.24.84 | 161 | established | UDP |
| 210.99.201.14 | 2001 | 129.63.24.87 | 80 | established | TCP |
| 24.102.129.21 | 3389 | 129.63.24.87 | 110 | established | TCP |

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc có trạng thái

- Bộ lọc có trạng thái và bộ lọc phi trạng thái thường được sử dụng kết hợp với nhau. Khi gặp khó khăn trong việc xác định chặn một gói dựa trên trạng thái kết nối, ACL sẽ được sử dụng để giúp ra quyết định chính xác.
- Việc giữ lại các trạng thái kết nối cần đến các cấu trúc dữ liệu phức tạp và các giải thuật tìm kiếm. Thực hiện những công việc này đòi hỏi không gian lưu trữ lớn, hoạt động nhiều hơn của CPU, giảm lưu lượng mạng.

2. Bộ lọc gói tin (Packet Filters)

Bộ lọc có trạng thái

- Attacker có thể đưa một số lượng lớn các gói tin vào tường lửa mục tiêu sử dụng bộ lọc có trạng thái, có thể làm ngắt các kết nối giữa mạng nội bộ và bên ngoài.
- Do đó, khi sử dụng bộ lọc có trạng thái, cần phải chắc chắn rằng có thể quản lý được sự phức tạp giữa thời gian và không gian. Ví dụ, thay vì giữ lại toàn bộ thông tin lịch sử của một kết nối, chỉ cần giữ lại thông tin của kết nối này trong một khoảng thời gian nào đó.

3. Cổng mạch (Circuit Gateways)

Khái niệm chung

- Cổng mạch (Circuit gateways, còn gọi là Circuit-level gateways), thực thi tại tầng vận chuyển (đôi khi có ngoại lệ).
- Thường kết hợp các bộ lọc gói tin và cổng mạch để tạo ra một bộ lọc gói tin động (Dynamic Packet Filter – DFD).

3. Cổng mạch (Circuit Gateways)

Cấu trúc cơ bản

- Đối tượng của cổng mạch là chuyển tiếp một kết nối TCP giữa một host nội bộ và một host bên ngoài. Do đó, cổng mạch cũng được xem như là một Transparent Proxy Firewall.
 - Trước tiên, cổng mạch sẽ xác nhận một phiên TCP (hoặc UDP).
 - Kế đó cổng mạch thực thi riêng biệt một kết nối với host nội bộ và một kết nối với host bên ngoài.
 - Duy trì một bảng các kết nối hợp lệ và duy trì việc kiểm tra các gói tin đi vào với các thông tin chứa trong bảng.
 - Cho phép gói tin đi qua nếu thuộc về một kết nối đã có duy trì trong bảng, ngược lại sẽ bị chặn.
 - Khi phiên kết thúc, entry tương ứng sẽ bị huỷ khỏi bảng và mạch được đóng lại.

3. Cổng mạch (Circuit Gateways)

Cấu trúc cơ bản

- Trong thực tế, một tổ chức thường phân tách mạng nội bộ của mình với mạng ngoại vi bằng một cổng mạch có một địa chỉ IP public có thể kết nối với ngoại vi, và các host trong mạng nội bộ sử dụng địa chỉ IP private không thể vươn tới được từ Internet.
- Sau khi thực thi một kết nối mạng với host ngoại vi và một kết nối mạng với host nội bộ, cổng mạch sẽ đóng vai trò như là một node chuyển tiếp mà không cần kiểm tra các gói tin đi qua nó. Do đó, một user nội bộ có thể mở một port trên một host nội bộ và chỉ thị cho gateway thực thi kết nối giữa host ngoại vi và host nội bộ.

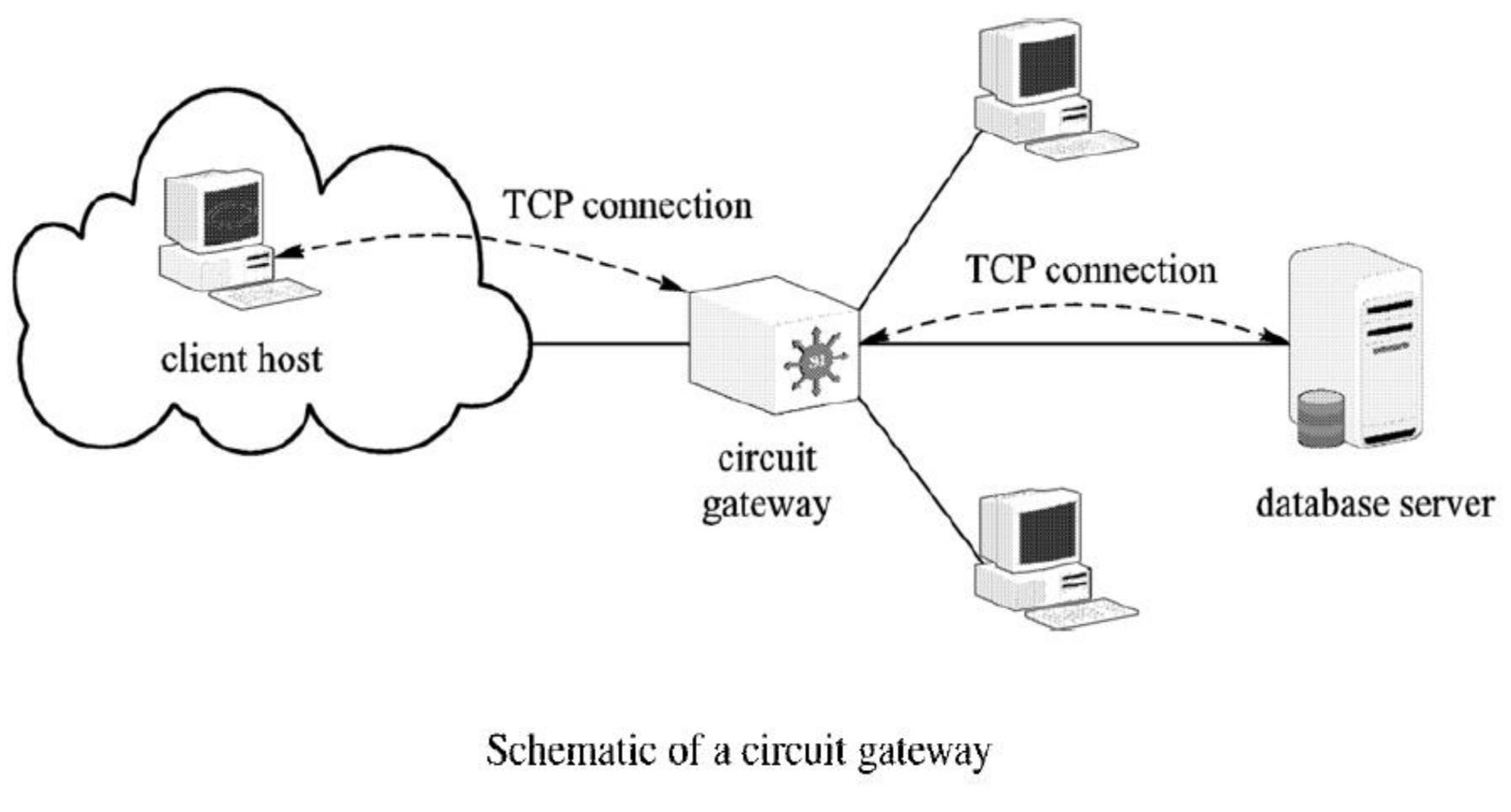
3. Cổng mạch (Circuit Gateways)

Cấu trúc cơ bản

- Do đó, các gói tin độc hại có thể vào mạng nội bộ qua một kênh đã thiết lập sẵn. Vì vậy, cổng mạch nên được sử dụng cùng với các bộ lọc gói tin.
- Cổng mạch nên sử dụng một tập tin log để ghi nhận lại thông tin của các gói tin (vào, ra) đã xác nhận, bao gồm địa chỉ IP nguồn, port nguồn, địa chỉ IP đích, port đích, và chiều dài của mỗi gói tin. File log này có thể giúp cho việc nhận định các vấn đề phát sinh về sau.

3. Cổng mạch (Circuit Gateways)

Cấu trúc cơ bản



4. Công ứng dụng (Application Gateways)

Khái niệm chung

Chức năng của Proxy đại diện để tải đi sang các web khác

- Còn được gọi là Application-level gateways (ALG) hay **Proxy Servers**, là các gói phần mềm được cài đặt trên một máy tính được chỉ định.
- Một ALG hoạt động như một proxy cho một host nội bộ, xử lý các dịch vụ được yêu cầu bởi các clients ngoại vi.
- Một ALG thực thi các kiểm tra chi tiết trên mỗi gói IP (vào, ra), bao gồm việc kiểm tra những định dạng chương trình ứng dụng (ví dụ như định dạng MIME, định dạng SQL...) chứa trong gói và xem xét payload của nó có được cho phép hay không.

4. Công ứng dụng (Application Gateways)

Cache Gateways

- Giả sử một tổ chức muốn cài đặt một Web server và cho phép các user hợp pháp trên Internet có thể truy cập đến các trang Web này trên Web server.
- Để bảo vệ Web server khỏi bị tổn hại, một phương án phổ biến là cài đặt một công ứng dụng như là một proxy cho Web server này, gọi là Web proxy server.
- Web proxy server nhận các yêu cầu tại cổng 80 từ các client ngoại vi và thực hiện kiểm tra chi tiết phần payload của gói tin.
- Chỉ sau khi phần payload này thoả yêu cầu kiểm tra, Web proxy server sẽ chuyển gói này đến Web server.

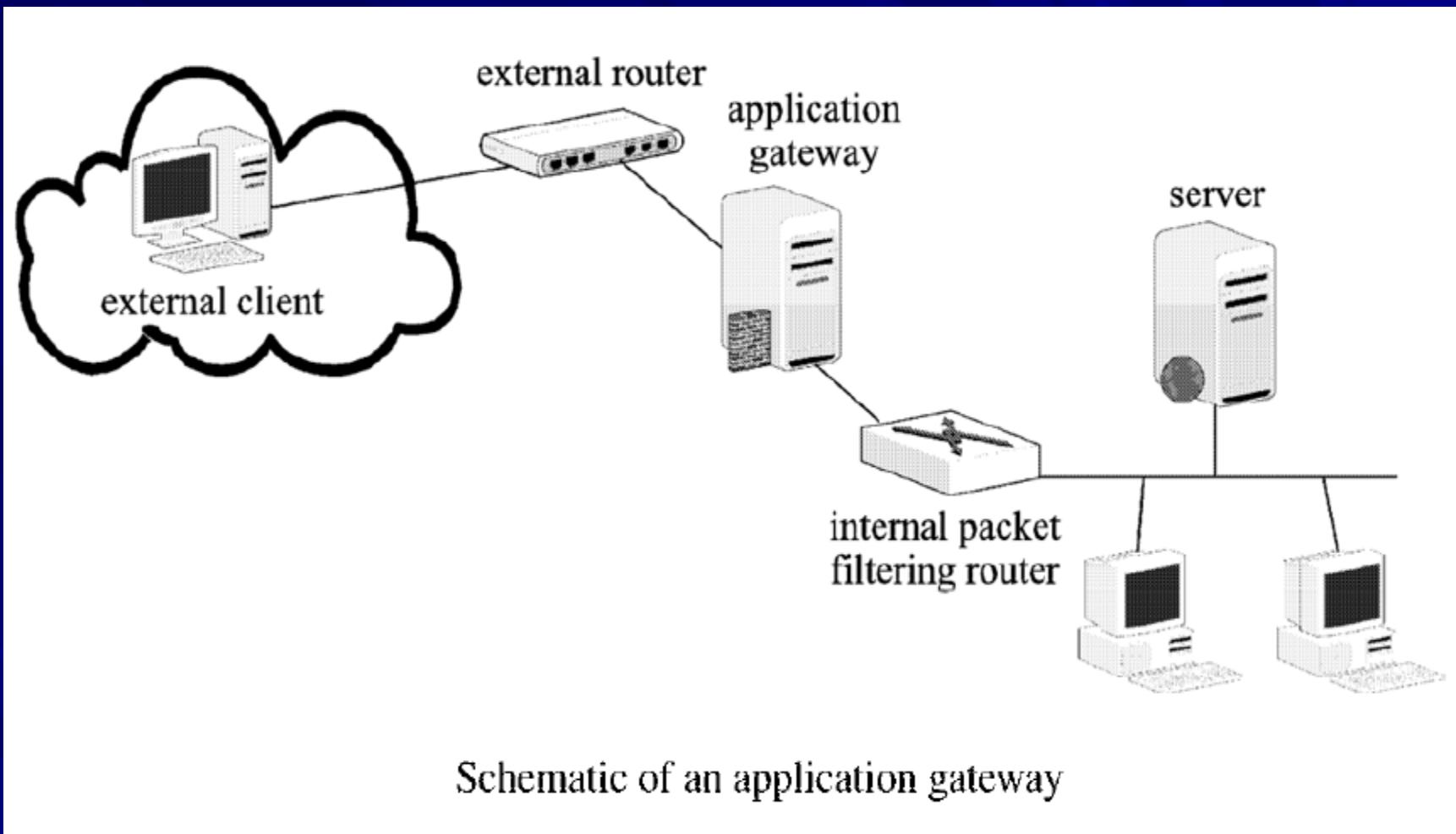
4. Cổng ứng dụng (Application Gateways)

Cache Gateways

- Web proxy server cũng kiểm tra các trang Web do Web server gửi đến các client ngoại vi và lưu chúng trong cache của nó.
- Nếu các client khác cũng yêu cầu những trang Web này, Web proxy server sẽ chuyển trực tiếp các trang này từ cache đến client mà không cần truy cập đến Web server.
- Loại Web proxy server này còn được gọi là cổng ứng dụng (Cache Gateways).
- Một cổng ứng dụng thường sử dụng với một router có khả năng lọc gói tin. Router này được đặt phía sau gateway để bảo vệ các kết nối giữa gateway và các host nội bộ.

4. Công ứng dụng (Application Gateways)

Cache Gateways



5. Bastion Hosts

- Một cổng ứng dụng là một máy tính đặt giữa mạng nội bộ và mạng ngoại vi nên dễ bị tấn công bởi attackers từ Internet. Do đó, các máy tính này cần sự bảo vệ nghiêm ngặt để trở thành bastion hosts.
- Bastion hosts là các máy tính với cơ chế phòng thủ mạnh. Chúng thường được dùng làm cổng ứng dụng, cổng mạch, hoặc các kiểu tường lửa khác.
- Một bastion host được cài đặt với một hệ điều hành tin cậy và không chứa những chương trình hoặc chức năng không cần thiết nhằm giảm đi những lỗi không đáng có và dễ dàng kiểm tra tính bảo mật.

5. Bastion Hosts

- Gateways hoạt động trên bastion hosts cần phải thoả những điều kiện:
 1. Phần mềm Gateway chỉ nên viết theo những module nhỏ để dễ dàng cho việc kiểm tra.
 2. Một bastion host cần chứng thực các user tại tầng mạng bằng cách xác nhận địa chỉ IP nguồn và đích chứa trong gói IP. Gateways chạy trên bastion host nên chứng thực user độc lập tại một tầng cao hơn.
 3. Một bastion host chỉ nên kết nối đến một số lượng nhỏ những host nội bộ.

5. Bastion Hosts

4. Bastion hosts nên giữ lại các file log, lưu trạng thái của mỗi phiên TCP để giúp admin xác định được các vấn đề phát sinh.
5. Nếu nhiều gateways đang chạy trên một bastion host đơn, những gateways này cần phải được xử lý một cách độc lập. Nếu một gateway bị lỗi, admin có thể shutdown nó mà không ảnh hưởng đến các gateways khác.
6. Bastion hosts nên hạn chế ghi dữ liệu lên đĩa cứng của chúng nhằm giảm cơ hội các mã độc hại xâm nhập vào hệ thống.
7. Gateways chạy trên một bastion host không nên được dùng quyền admin hệ thống.

6. Cấu hình tường lửa

Khái niệm chung

- Gateways chạy trên một bastion host thường được sử dụng với bộ lọc gói tin.
- Các cấu hình tường lửa thông dụng:
 - Single-Homed Bastion Host System (SHBH)
 - Dual-Homed Bastion Host System (DHBH)
 - Screened Subnets (SS)
 - Demilitarized Zones (DMZ)

6. Cấu hình tường lửa

Single-Homed Bastion Host System

- Bao gồm một packet-filtering router và một bastion host, trong đó router kết nối mạng nội bộ với mạng ngoại vi và bastion host nằm trong mạng nội bộ.
- Router sẽ thông báo ra bên ngoài địa chỉ IP và số port của các server nội bộ.
- Router sẽ không chuyển tiếp các gói tin đi vào trực tiếp đến các server mà sẽ kiểm tra các gói tin này, sau đó mới chuyển cho bastion host.
- Bastion host tiếp tục kiểm tra gói tin đi vào, nếu thỏa, sẽ xác định server nội bộ nào gói tin muốn được chuyển tới.

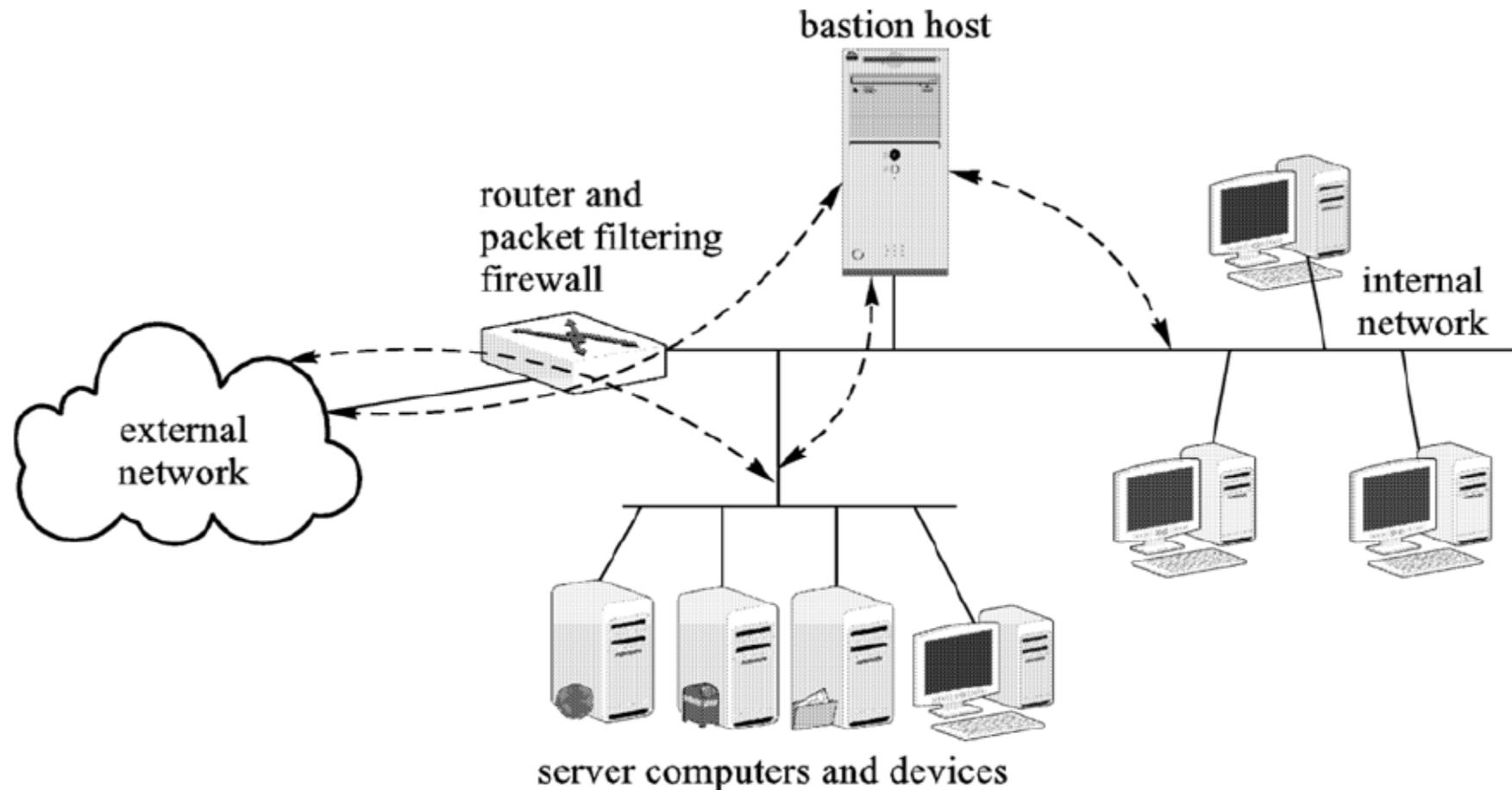
6. Cấu hình tường lửa

Single-Homed Bastion Host System

- Các gói tin từ mạng nội bộ đi ra bên ngoài cũng phải qua bastion host. Bộ lọc gói tin của tường lửa kiểm tra mỗi gói tin đi ra ngoài và ngăn lại nếu địa chỉ nguồn của nó không phải là địa chỉ IP của bastion host hoặc không thoả các quy tắc lọc.
- Trong một hệ thống SHBH, nếu attacker thoả hiệp được với packet-filtering router thì có thể sửa được các luật trong ACL để bỏ qua bastion host và truyền thông trực tiếp với các host nội bộ. Vấn đề này có thể giải quyết bằng cách sử dụng Dual-Home Bastion Host (DHBH).

6. Cấu hình tường lửa

Single-Homed Bastion Host System



Schematic of a single-homed bastion host network, where the dotted arrow lines show the actual communications and the solid lines show the physical network connections

6. Cấu hình tường lửa

Dual-Homed Bastion Host System

- Một DHBH chia mạng nội bộ vào hai zones: inner zone (private zone) và outer zone.
- Địa chỉ IP của các host trong inner zone không thể vươn tới được từ các mạng ngoại vi.
- Địa chỉ IP của các host trong outer zone có thể vươn tới được trực tiếp từ các mạng ngoại vi.
- Router được đặt giữa mạng ngoại vi và outer zone, giữa mạng ngoại vi và bastion host.
- Inner zone trong DHBH chỉ được kết nối đến bastion host nên được bảo vệ bởi cả bastion host và packet-filtering router.

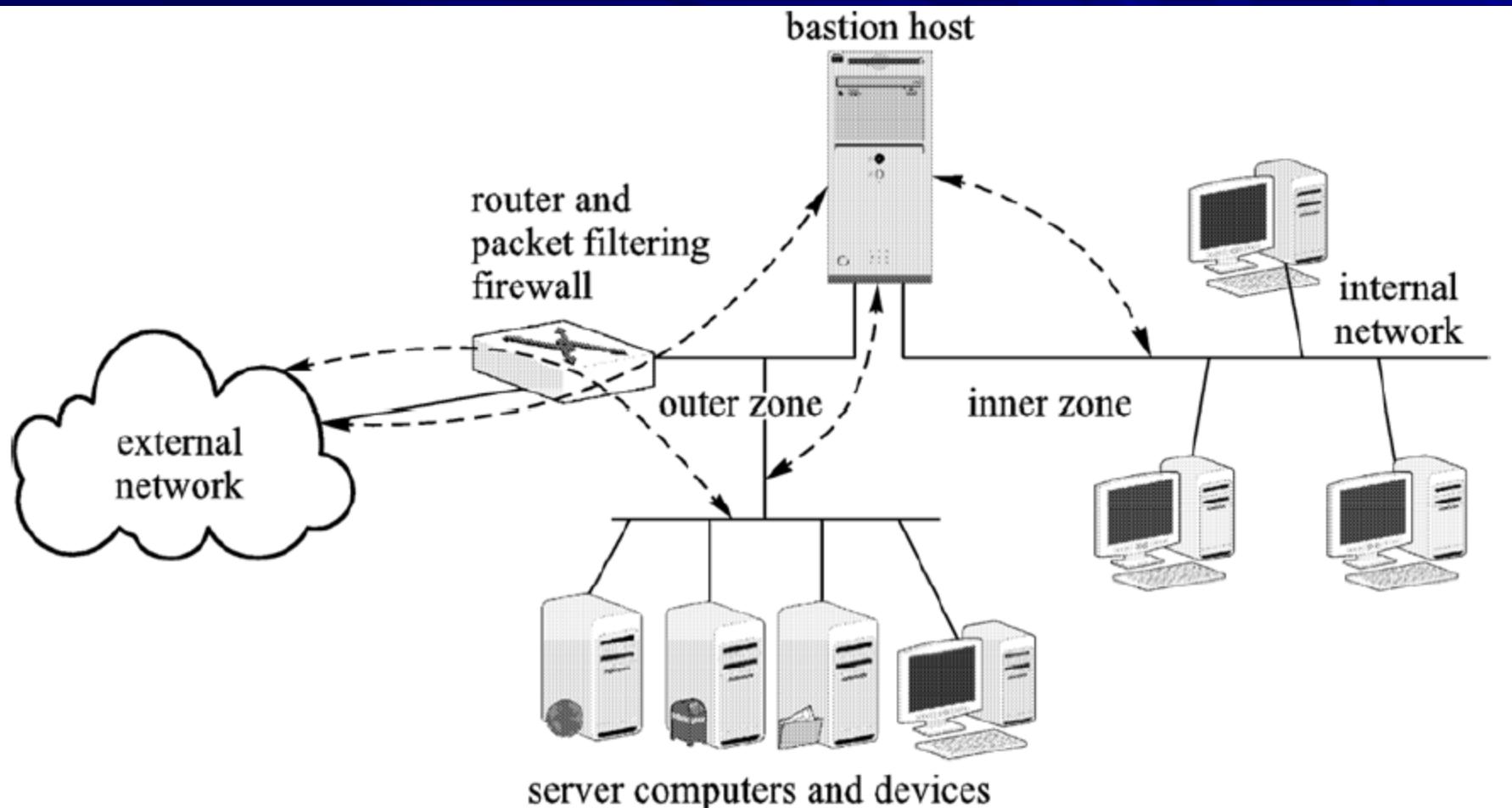
6. Cấu hình tường lửa

Dual-Homed Bastion Host System

- Các server trong outer zone được bảo vệ bởi packet-filtering router.
- Tương tự như trong hệ thống SHBH, một DHBH cho phép các máy tính server trong outer zone có thể được truyền thông trực tiếp đến Internet mà không cần phải đi qua bastion host.
- ACL trong router cho phép các gói từ ngoài vào đi qua nó nếu địa chỉ nguồn được cho phép, và địa chỉ IP đích cùng số port thỏa với địa chỉ IP của máy server cũng như một port đang mở của server này.
- Trong hệ thống DHBH, attacker nếu thỏa hiệp với packet-filtering router cũng vẫn không thể vượt qua được bastion host.

6. Cấu hình tường lửa

Dual-Homed Bastion Host System



Schematic of a dual-homed bastion host network, where the dotted arrow lines show the actual communications and the solid lines show the physical network connections

6. Cấu hình tường lửa

Screened Subnets

- Là cấu hình tường lửa bảo mật nhất.
- Bao gồm một bastion host và hai packet-filtering router (là một mạng SHBH với packet-filtering router thứ hai (inner router) chen vào giữa bastion host và mạng nội bộ).
- Nói cách khác, trong một Screened Subnet, một router đặt giữa Internet và bastion host, một router khác đặt giữa bastion host và mạng nội bộ.
- Hai tường lửa lọc gói sẽ tạo ra một screened subnetwork cô lập ở giữa. Các máy tính server và thiết bị nào không cần bảo mật mạnh thường được đặt trong screened subnetwork này.

6. Cấu hình tường lửa

Screened Subnets

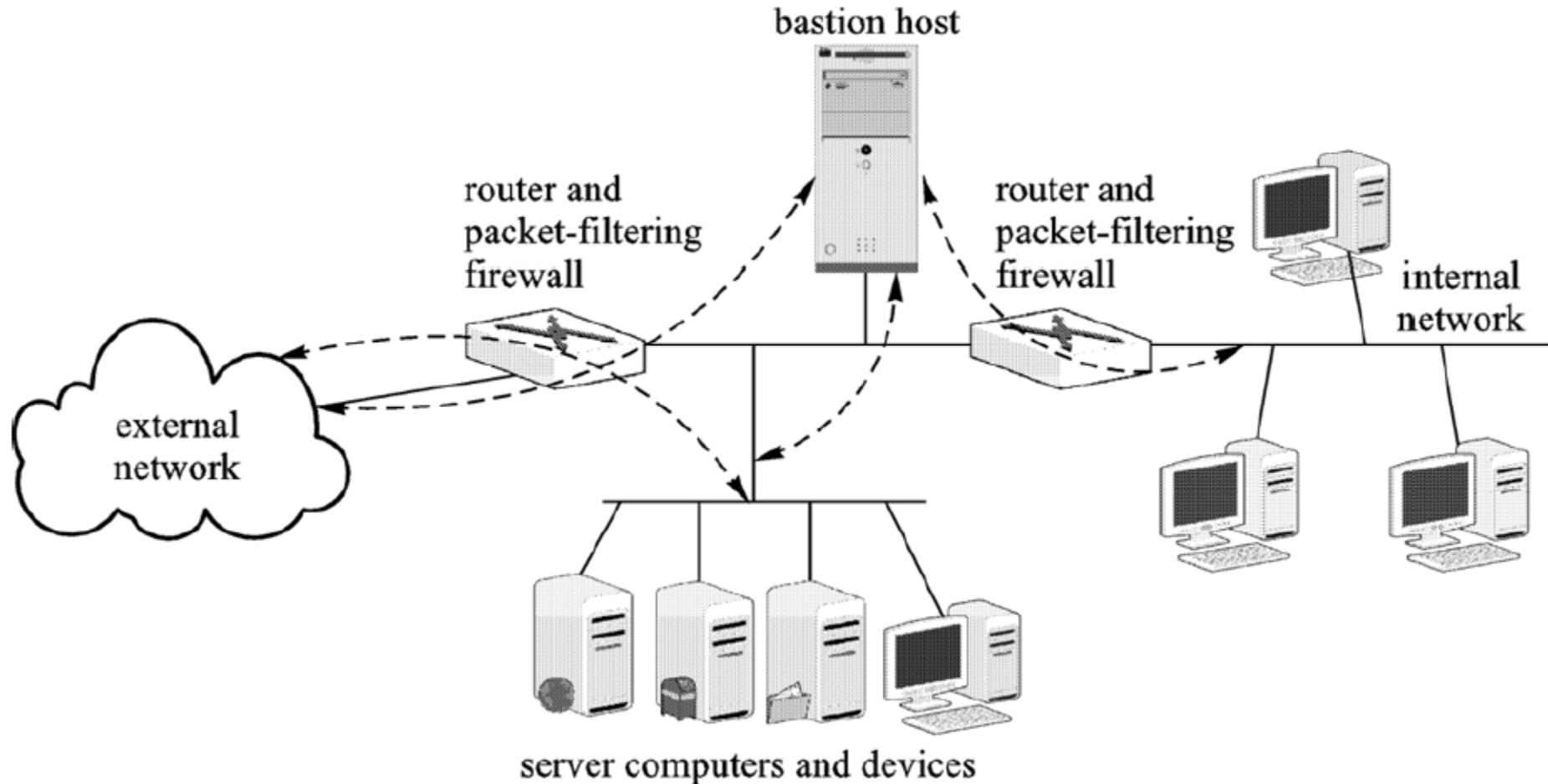
- Router ngoài (outer router) sẽ thông báo cho mạng ngoại vi địa chỉ IP và số port của các máy tính server và thiết bị kết nối đến screened subnetwork.
- Router trong (inner router) sẽ thông báo cho mạng nội bộ địa chỉ IP và số port của các máy tính server và thiết bị kết nối đến screened subnetwork.
- Cấu trúc của mạng nội bộ là ẩn với thế giới bên ngoài.
- Có thể di chuyển một số server (database server...) từ screened subnetwork đến mạng nội bộ để cung cấp một sự bảo vệ mạnh hơn.

6. Cấu hình tường lửa Screened Subnets

- Có thể đặt các proxy server tương ứng (chẳng hạn database server) trong screened subnetwork.
- Cấu hình này làm tăng tính bảo mật của hệ thống nhưng cũng làm giảm tốc độ xử lý nên trong mỗi ứng dụng cụ thể, cần tìm kiếm những cấu hình tối ưu phù hợp.

6. Cấu hình tường lửa

Screened Subnets



Schematic of a screened subnet system, where the dotted arrow lines show the actual communications and the solid lines show the physical network connections

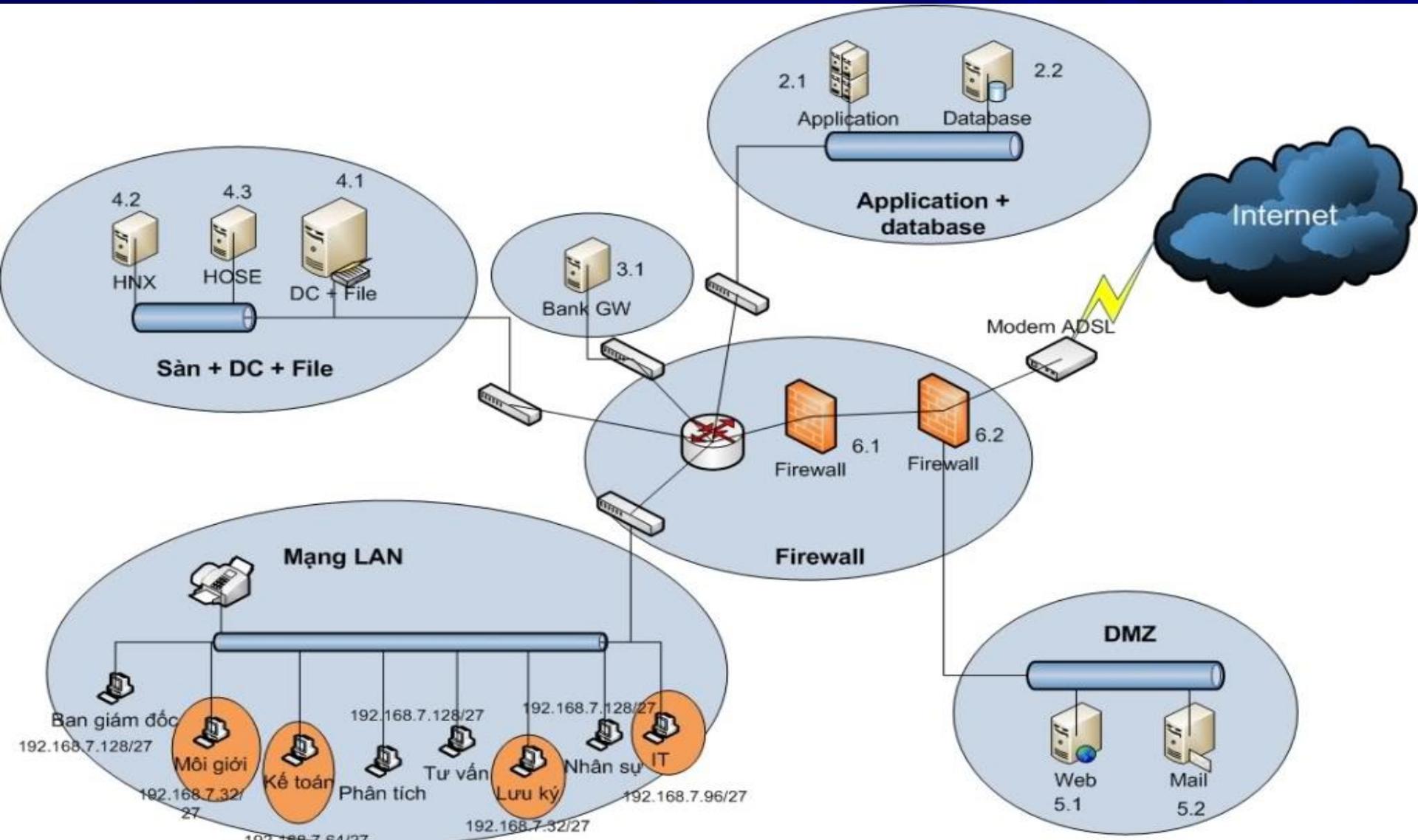
6. Cấu hình tường lửa

Demilitarized Zones (DMZ)

- Một subnet giữa hai tường lửa trong mạng nội bộ thường được xem như một Demilitarize zone (DMZ).
- Tường lửa bên ngoài bảo vệ vùng DMZ với mạng ngoại vi và tường lửa bên trong bảo vệ mạng nội bộ với vùng DMZ.
- Một DMZ có thể có hoặc không có bastion host.
- Các server không yêu cầu bảo mật mạnh được đặt trong vùng DMZ.
- Các máy tính cần phải được bảo mật cao nhất được đặt trong subnet kết nối đến tường lửa bên trong.

6. Cấu hình tường lửa

Demilitarized Zones (DMZ)



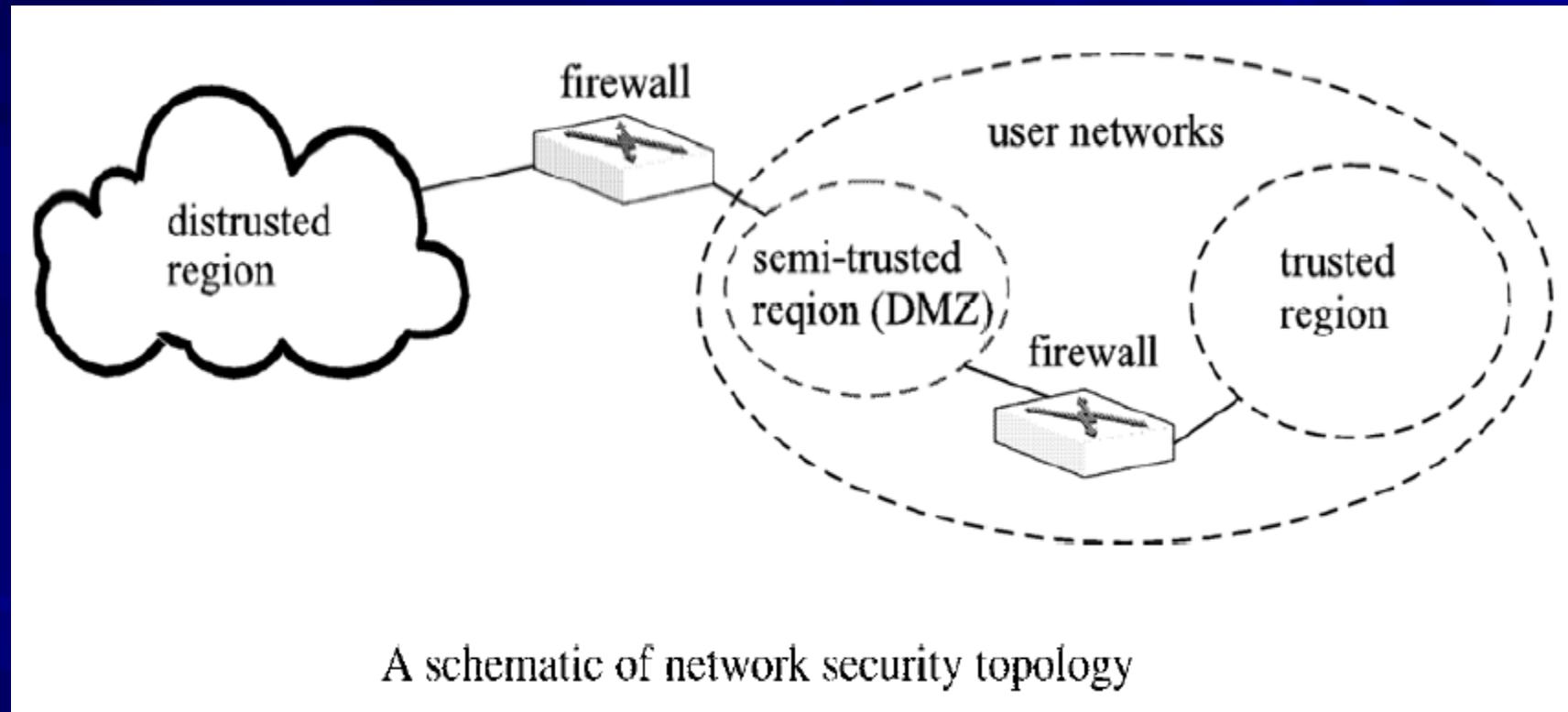
6. Cấu hình tường lửa

Network Security Topology

- Tường lửa có thể sử dụng để chia mạng thành ba vùng phân biệt:
 - Vùng không tin cậy: là mạng ngoại vi bên ngoài của tường lửa ngoài.
 - Vùng kém tin cậy: là vùng DMZ nằm giữa tường lửa ngoài và tường lửa trong.
 - Vùng tin cậy: là mạng nội bộ nằm đằng sau tường lửa trong.

6. Cấu hình tường lửa

Network Security Topology



7. Chuyển dịch địa chỉ mạng

- NAT (Network Address Translation Protocol) chia địa chỉ IP vào hai nhóm.
 - Nhóm 1 bao gồm các địa chỉ IP công cộng, có thể vươn tới được từ mạng ngoại vi.
 - Nhóm 2 bao gồm các địa chỉ IP riêng và không thể vươn tới được một cách trực tiếp từ mạng ngoại vi.
- Xem lại NAT tĩnh, NAT động, PAT, VLAN trong môn Thiết bị mạng.

8. TMG – Threat Management Gateway

Forefront Threat Management Gateway 2010 là phiên bản của Microsoft thay thế cho ISA 2006.

The screenshot shows the Microsoft Forefront Threat Management Gateway 2010 (TMG) management console. The left sidebar contains a navigation tree with options like Dashboard, Monitoring, Firewall Policy, Web Access Policy, E-Mail Policy, Intrusion Prevention System, Remote Access Policy (NAP), Networking, System, Logs & Reports, Update Center, and Troubleshooting. The main area displays the 'All Firewall Policy' screen, which lists 12 rules. The columns include Order, Name, Action (Allow or Deny), Protocols (HTTP, HTTPS, PPTP, etc.), and From / Listener and To addresses. Rule 1 (OWA(1)) is selected. A message at the top right says, 'To save changes and update the configuration, click Apply.' On the right side, there are two panels: 'Firewall Policy Tasks' and 'Policy Editing Tasks'. The 'Firewall Policy Tasks' panel includes options like Publish Exchange Web Client Access, Publish Mail Servers, Publish SharePoint Sites, Publish Web Sites, Publish Non-Web Server Protocols, Create Access Rule, Configure VoIP, and Configure Client Access. The 'Policy Editing Tasks' panel includes Edit Selected Rule, Delete Selected Rules, Move Selected Rules Down, and Disable Selected Rules.

| Order | Name | Action | Protocols | From / Listener | To |
|-------|---------------------|--------|-----------------------|------------------|----------------|
| 1 | OWA(1) | Allow | HTTP, HTTPS | 121 - HTTPS | exchange.co... |
| 2 | OWA | Allow | HTTP, HTTPS | 121 - HTTPS | exchange.co... |
| 3 | Allow from DC | Allow | All Outbound... | DC1.contoso... | Local Host |
| 4 | RDP Server | Allow | RDP (Terminal...) | External | 10.1.1.1 |
| 5 | FTP | Allow | FTP Over HTTP, FTP | Internal | Anywhere |
| 6 | Allow PPTP Outba... | Allow | PPTP | Internal | Anywhere |
| 7 | VPN +HTTP No Pr... | Allow | HTTP -No Proxy, HTTPS | VPN Clients | Internal |
| 8 | DNS Server | Allow | DNS Server | External | 10.1.1.1 |
| 9 | SMTP SMTP Server | Allow | SMTP Server | External | 10.1.1.10 |
| 10 | Allow DNS | Allow | DNS | DC1.contoso... | External |
| 11 | Autodiscover | Allow | HTTPS | 123 - Autodis... | exchange.co... |
| 12 | Outlook Anywhere | Allow | HTTPS | 122- OA | exchange.co... |

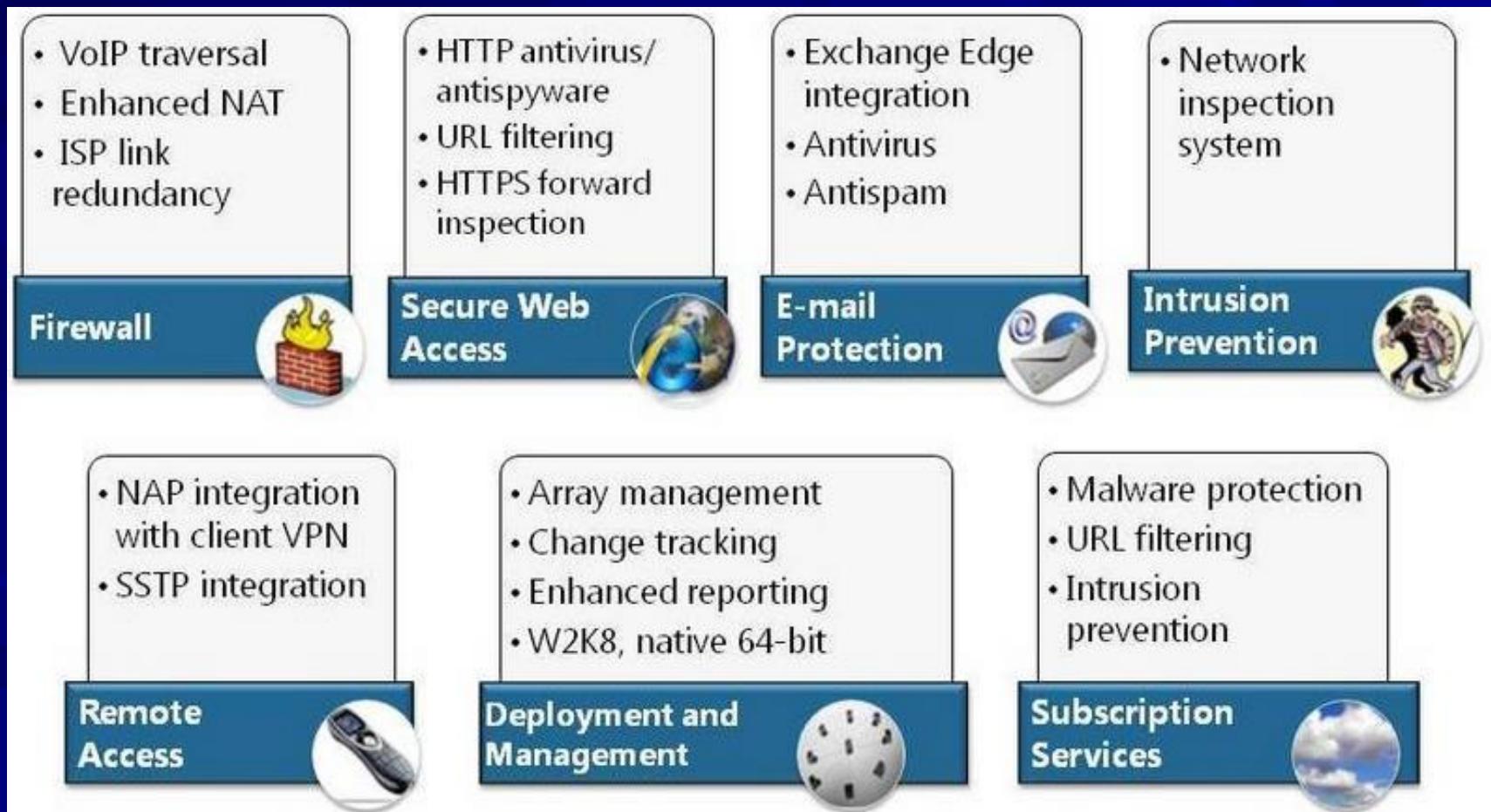
8. TMG – Threat Management Gateway

1. Yêu cầu cài đặt

| | Minimum | Recommended |
|------------------|---|---|
| Processor | 2 core (1 CPU x dual core) 64-bit processor | 4 core (2 CPU x dual core or 1 CPU x quad core) 64-bit processor |
| Memory | 2 gigabytes (GB) of memory | 4 gigabytes (GB) of memory |
| Hard Disk Space | 2.5 GB of available hard disk space* | 2.5 GB of available hard disk space* |
| Hard Disks | One local hard disk partition formatted with NTFS | Two disks for system and logging, and one for caching and malware inspection |
| Network | One network adapter for communicating with the internal network | One network adapter for each network connected to the Forefront TMG 2010 server |
| Operating System | Windows Server® 2008 x64 with Service Pack 2, or Windows Server® 2008 R2 | |

8. TMG – Threat Management Gateway

2. Tính năng chính của TMG



8. TMG – Threat Management Gateway

3. Các điểm mới của TMG so với ISA

| | ISA Server 2006 | Forefront TMG |
|--|--------------------|------------------|
| Network layer firewall | ✓ | ✓ |
| Application layer firewall | ✓ | ✓ |
| Internet access protection (proxy) | ✓ | ✓ |
| Basic OWA and SharePoint publishing | ✓ | ✓ |
| Exchange publishing (RPC over HTTP) | ✓ | ✓ |
| IPSec VPN (remote and site-to-site) | ✓ | ✓ |
| Web caching, HTTP compression | ✓ | ✓ |
| Windows Server® 2008 R2, 64-bit (only) | | ✓ New |
| Web antivirus, antimalware | | ✓ New |
| URL filtering | | ✓ New |
| E-mail antimalware, antispam | | ✓ New |
| Network intrusion prevention | | ✓ New |
| Enhanced UI, management, reporting | | ✓ New |

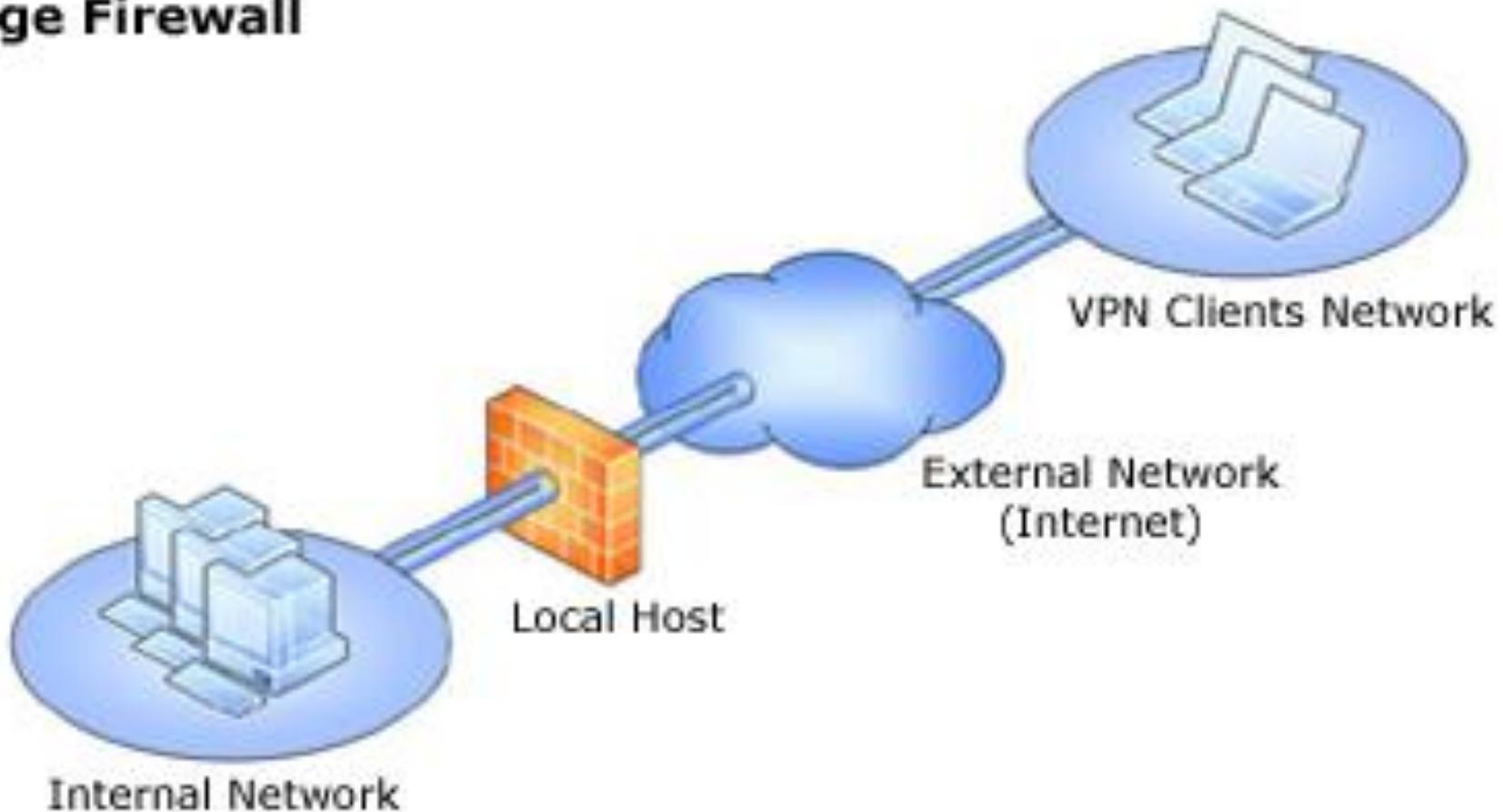
8. TMG – Threat Management Gateway

4. Các mô hình mạng trong TMG

- Edge Firewall
- 3-Leg Perimeter
- Front Firewall
- Back Firewall
- Single Network Adaptor

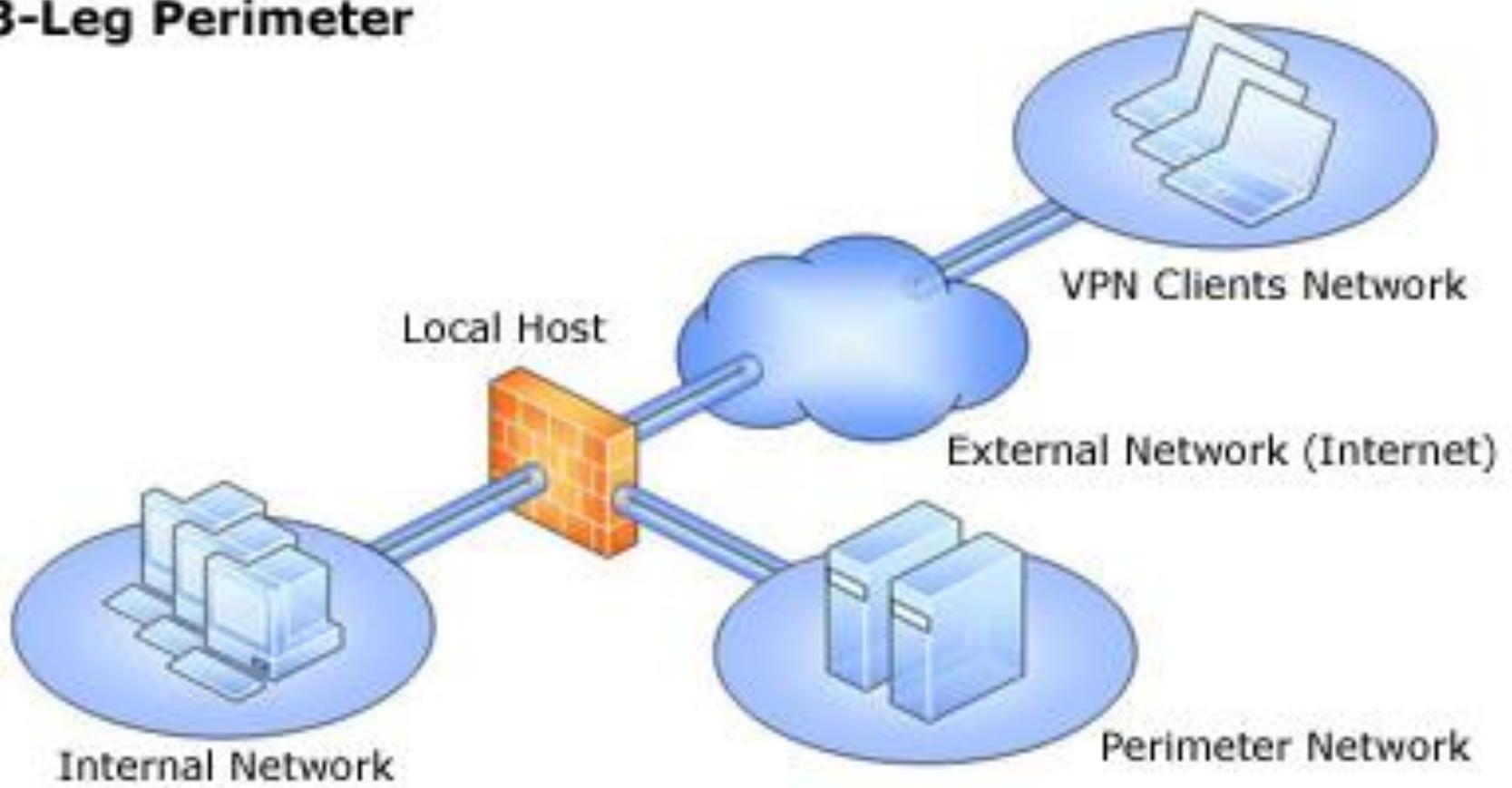
8. TMG – Threat Management Gateway

Edge Firewall

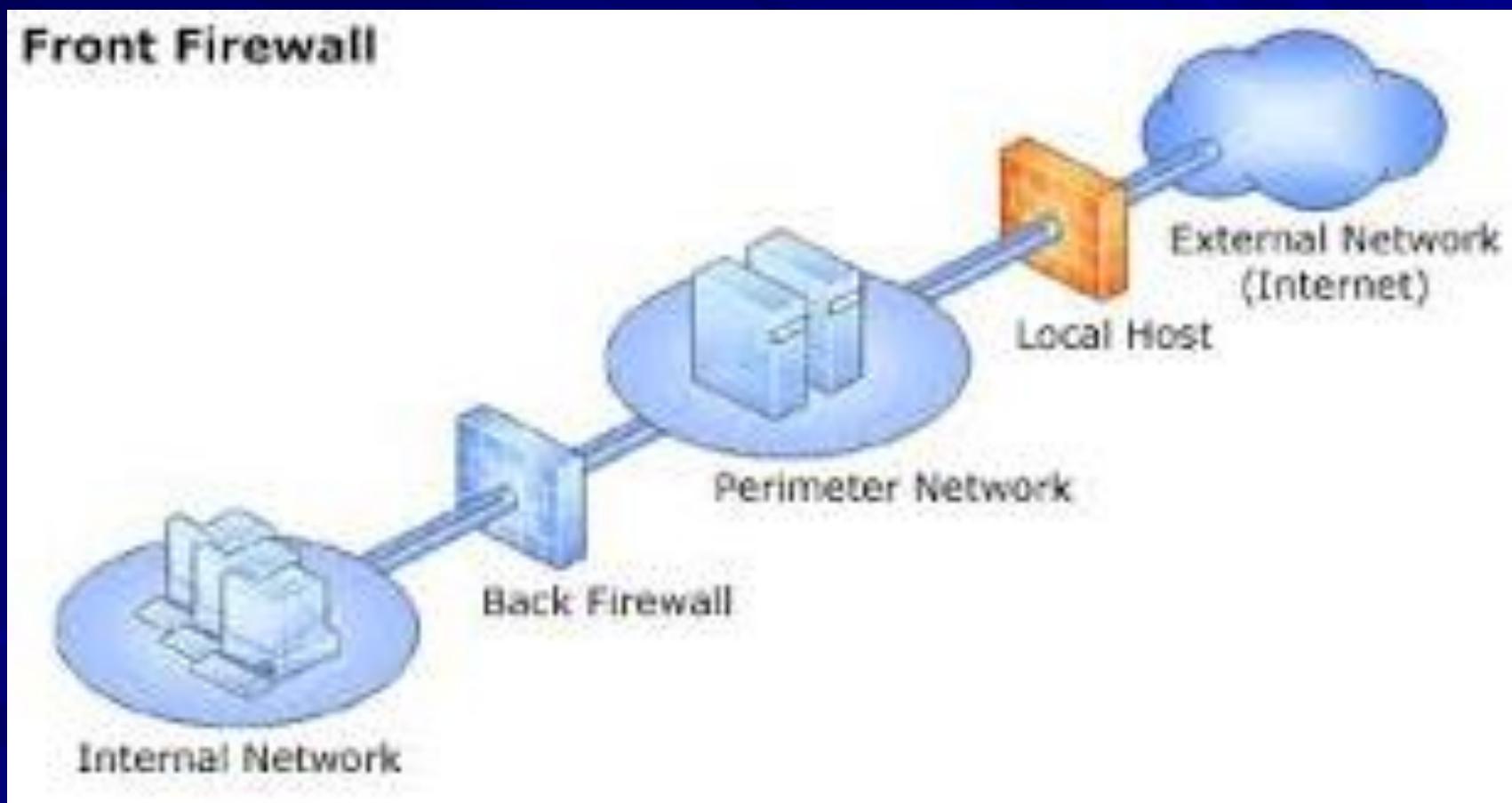


8. TMG – Threat Management Gateway

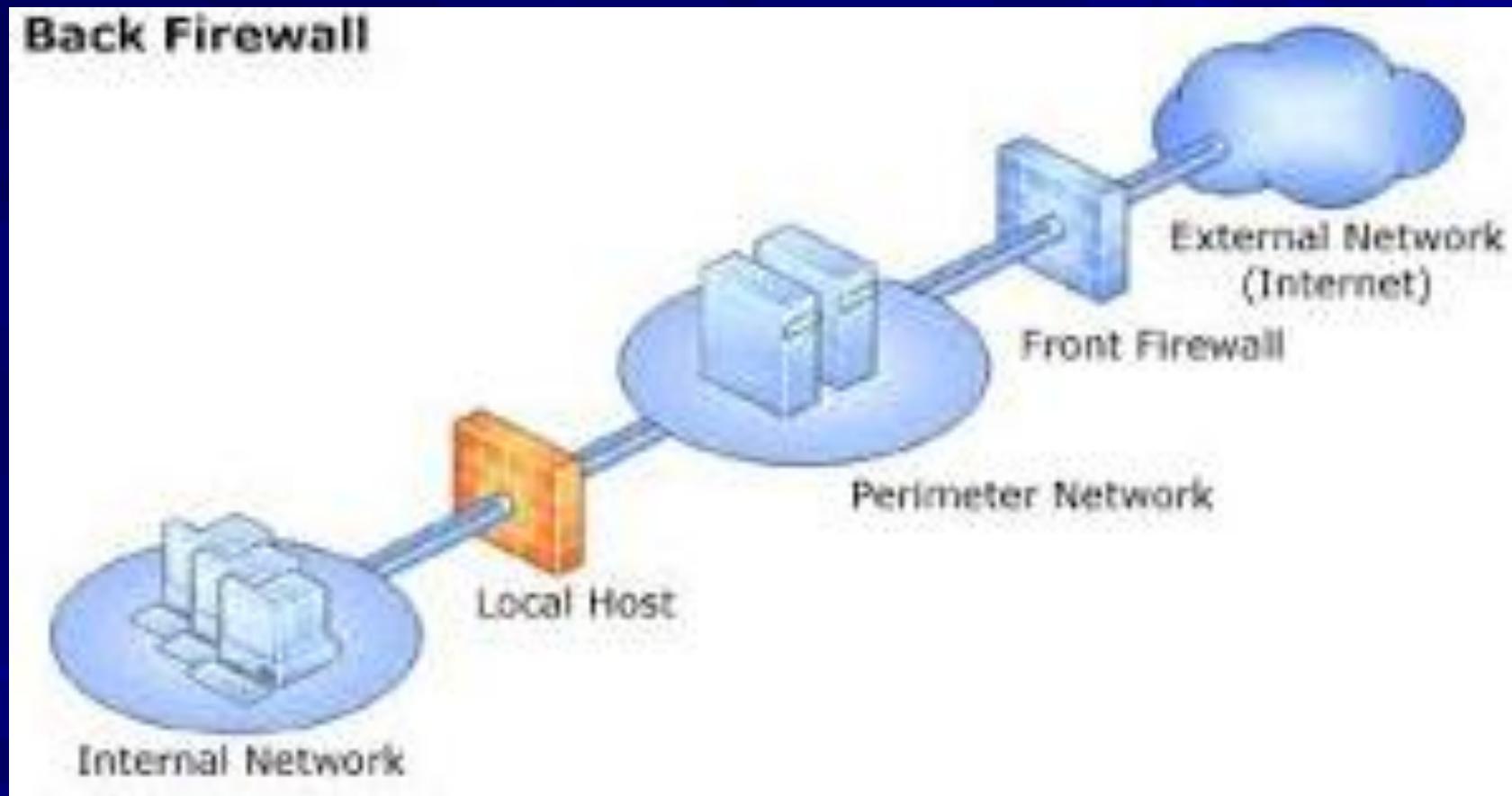
3-Leg Perimeter



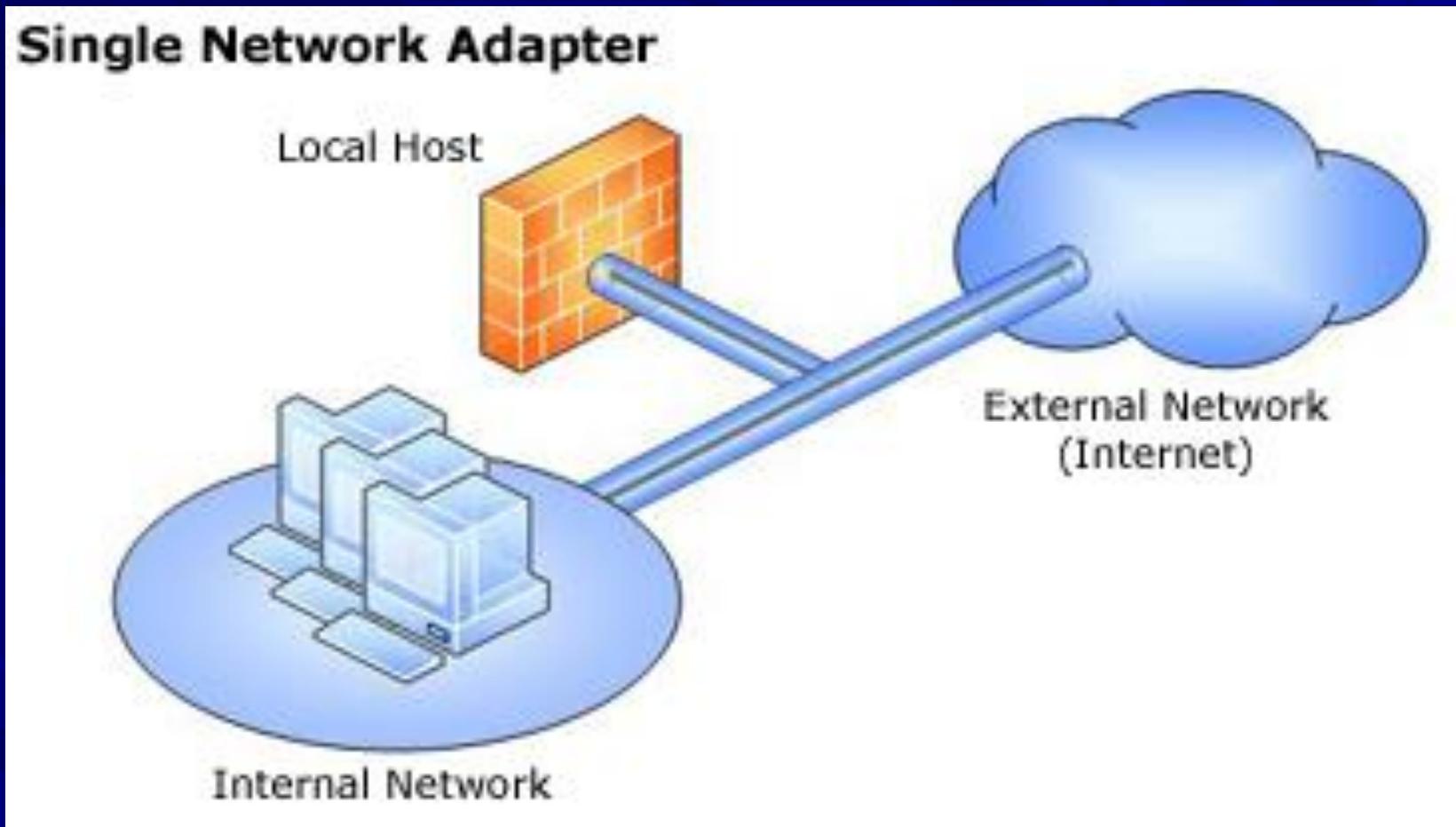
8. TMG – Threat Management Gateway



8. TMG – Threat Management Gateway



8. TMG – Threat Management Gateway



8. TMG – Threat Management Gateway

5. Cơ chế hoạt động

| Feature | SecureNAT Client | Forefront TMG Client | Web Proxy Client |
|---------------------------------------|---|---|---|
| Yêu cầu cài đặt | Không cần cài đặt, Client chỉ cần trỏ Default Gateway về TMG Server | Client phải cài chương trình Forefront TMG Client | Khai báo Proxy server trong các chương trình Web Browser (IE, Firefox...) |
| Hỗ trợ HĐH | Tất cả HĐH hỗ trợ TCP/IP | Chỉ hỗ trợ Windows | Tất cả Web Browser |
| Hỗ trợ các Protocol | Tất cả protocols | Tất cả protocols | Chỉ hỗ trợ HTTP, HTTPS, & FTP download |
| Hỗ trợ chứng thực User Account | Không | Có | Có |

9. Bài tập

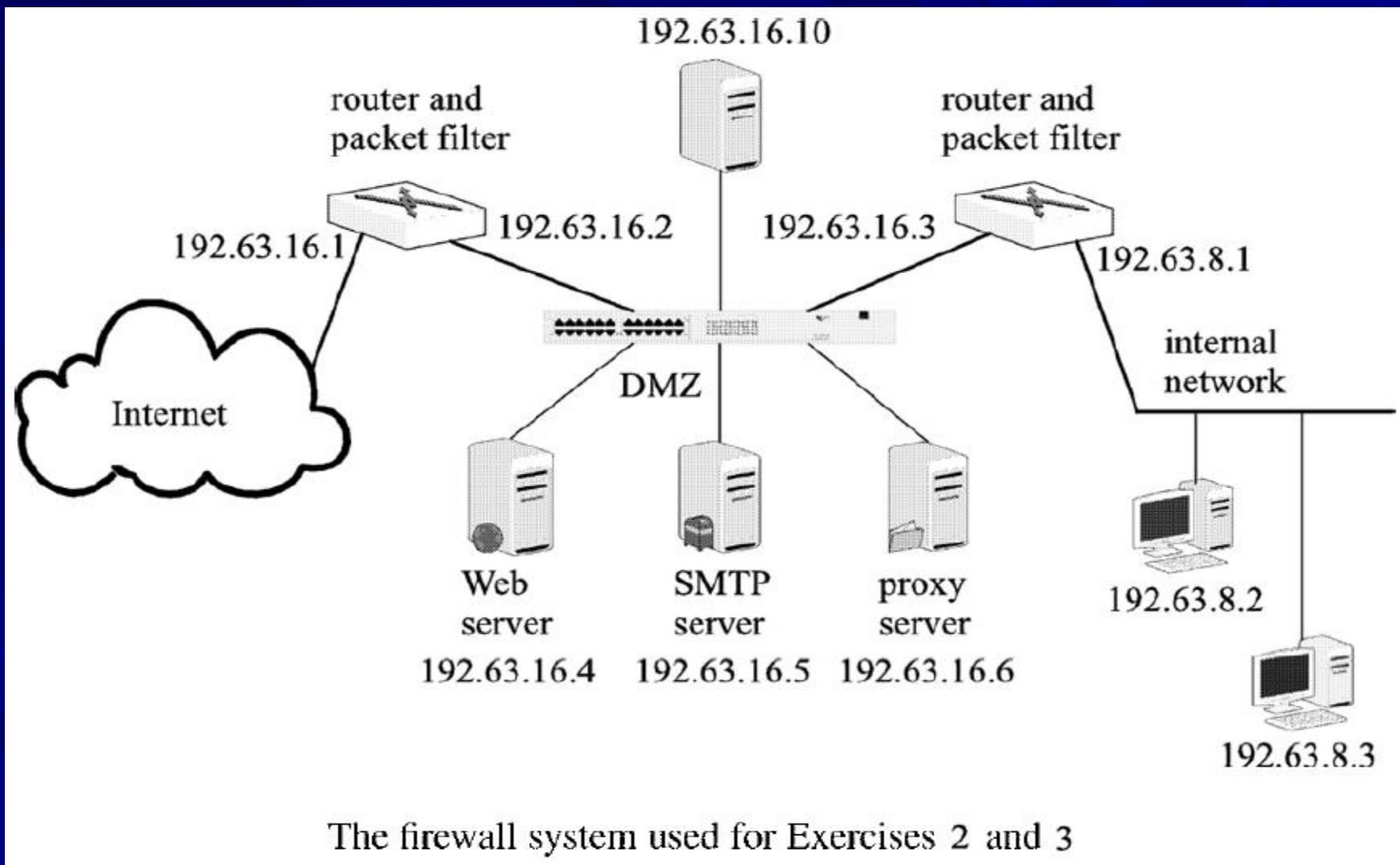
- Giả sử một ACL chứa những luật sau để xử lý các gói tin đi vào mạng:

| Int addr | Int port | ext addr | ext port | Action | Comments |
|----------|----------|----------|----------|--------|-------------------------------|
| * | 25 | * | * | allow | Allow ingress SMTP packets |

Luật này có hợp lý và có bảo mật?

- Giả sử trong sơ đồ của screened subnet mô tả trong hình dưới, chúng ta muốn nâng cao tính bảo mật của server SMTP. Hãy mô tả một hoặc nhiều phương pháp để giải quyết vấn đề này.

9. Bài tập



9. Bài tập

3. *Sử dụng sơ đồ mạng trong bài 2 để làm bài này:*

Vùng DMZ chứa 3 server. Địa chỉ IP của router ngoài, router trong và các server như trong hình. Xây dựng các luật ACL sao cho các host ngoại vi có thể trực tiếp truyền thông với các server trong vùng DMZ, nhưng không thể thực hiện truyền thông trực tiếp với bất kỳ host nào trong vùng mạng nội bộ.

9. Bài tập

4. Bảng dưới liệt kê các giao thức truyền thông chính sử dụng để thực thi các dịch vụ mạng cục bộ. Xây dựng các luật ACL để chặn các gói của những giao thức này đi ra mạng ngoại vi.

Communication protocols used for establishing LAN

| port | transport-layer protocol | application |
|--------------------|--------------------------|-------------|
| 67/68 | UDP | Bootp/DHCP |
| 69 | UDP | TFTP |
| 135, 137, 138, 139 | TCP and UDP | NetBIOS |
| 445 | TCP and UDP | CIFS |
| 515 | TCP | LPR |
| 2049 | UDP | NFS |

9. Bài tập

5. Nếu trong một gói tin từ mạng ngoại vi đi vào mạng nội bộ, địa chỉ nguồn của nó là một địa chỉ IP nội bộ hoặc là một địa chỉ IP riêng (private), gói này sẽ được cho phép hay sẽ bị chặn? Tại sao?
6. Nếu một gói đi vào có số port đích là 25 hoặc 80, gói này sẽ bị chặn hay không? Tại sao?
7. Nếu một gói đi vào có địa chỉ IP nguồn hoặc địa chỉ IP đích của nó là 0.0.0.0 thì bộ lọc có chặn gói này không? Tại sao? (Lưu ý: 0.0.0.0 là địa chỉ dành cho thông điệp broadcasting).

9. Bài tập

8. Luồng SMTP đi ra ngoài có bị lọc chặn không? Tại sao?
9. Một host nội bộ có được cho phép kết nối đến một server POP3/IMAP bên ngoài không? Tại sao?
10. Microsoft Windows sử dụng port từ 135 – 139 và 445 dành cho NetBIOS và chia sẻ file. Nếu một gói đi vào có 22 là số port của nó thì gói tin này có bị chặn không? Tại sao?

Thank You !