HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Bài 6. Một số công nghệ bảo mật

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

NỘI DUNG

1. Mục đích học
2. Điều khiển truy cập
3. Các hệ thống Bức tường lửa (Firewalls)
4. Truy cập từ xa và VPNs
5. Các hệ thống phát hiện, phòng chống xâm nhập (IDS/IPS)
6. Thảo luận, bài tập

1. Mục đích học

- Nhận ra vai trò quan trọng của việc điều khiển truy cập trong hệ thống, xác định và thảo luận các yếu tố xác thực
- Nắm bắt công nghệ bức tường lửa, các hướng triển khai bức tường lửa
- Xác thực và ủy quền người dùng truy cập từ xa
- Mô tả công nghệ cho phép sử dụng VPN
- Tìm hiểu về hệ thống phát hiện và ngăn ngừa bất thường

2. Điều khiển truy cập

2.1. Định nghĩa: là phương pháp mà một hệ thống xác định xem một người dùng có được thừa nhận ở 1 khu vực nhất định trong hệ thống hay không.

Ví dụ: người dùng sử dụng tài khoản, mật khẩu để đăng nhập vào 1 máy tính

2. Điều khiển truy cập

2.2. Phân loại:

i. Điều khiển truy cập bắt buộc (MAC): được dùng để bảo vệ dữ liệu cần được bảo mật cao trong một môi trường mà các dữ liệu và người dùng đều được phân loại rõ ràng

Ví dụ: để đọc file hệ thống, cần phải truy cập quyền root.

ii. Điều khiển truy cập tùy quyền (DAC): được thực hiện theo quyết định hoặc tùy chọn của người dùng dữ liệu

Ví dụ: sinh viên đăng nhập quyền **user**, phòng đào tạo đăng nhập quyền **admin** vào hệ thống quản lý điểm SV - RBAC, RDAC

2. Điều khiển truy cập

2.3. Các bước trong điều khiển truy cập:

i. Định danh (Identification): Người dùng cung cấp danh định tới hệ thống để xác thực. **Ví dụ**: người dùng cung cấp username, số điện thoại, email, …

ii. Xác thực (Authentication): Người dùng chứng minh danh định đó là đúng. **Ví dụ**: người dùng cung cấp mật khẩu, dấu vân tay, giọng nói,Số PIN ...

iii. Ủy quyền (Authorization): Xác định quyền mà người dùng có. **Ví dụ:** người dùng được sử dùng quền xem hoặc sửa hoặc xóa một tài nguyên nào đó của hệ thống.

3. Bức tường lửa (firewall)

3.1. Định nghĩa:

Là một **công nghệ** cho phép ngăn chặn các **thông tin** cụ thể di chuyển giữa bên trong và bên ngoài hệ thống

Bức tường lửa có thể là:

- Hệ thống máy tính hoặc một thiết bị riêng
- Dịch vụ phần mềm đang chạy trên bộ định tuyến hoặc máy chủ
- Mạng riêng chứa các thiết bị hỗ trợ

3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa: (cấu trúc)

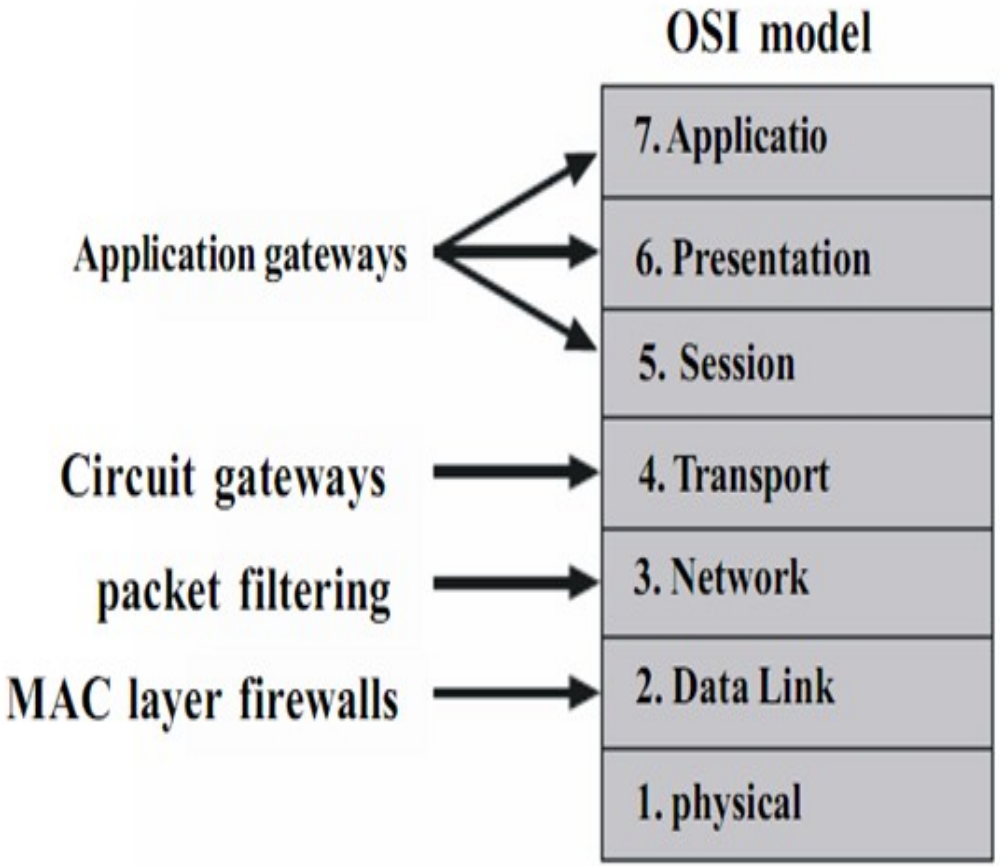
i. Packet filtering

ii. Application gateways

iii. Circuit gateways

iv. MAC layer firewalls

v. Hybrids

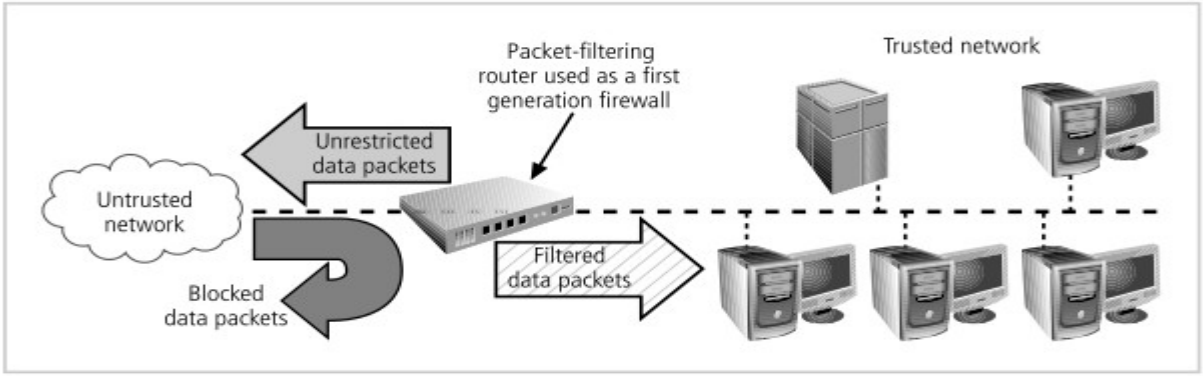


3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

i. **Packet filtering (Tường lửa lọc gói tin)**: là tường lửa kiểm tra thông tin tiêu đề (header) của gói tin

- Việc kiểm tra dựa trên sự kết hợp của IP nguồn, IP đích hoặc hướng di chuyển của gói tin (hướng vào, ra), hoặc dựa trên giao thức truyền tin TCP, UDP kết hợp kiểm tra các cổng được sử dụng
- Chế độ này sử dụng các quy tắc được thiết kế để cấm các gói với một số địa chỉ hoặc một phần địa chỉ nhất định



3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

i. Tường lửa lọc gói tin

Phân loại:

a) Lọc tĩnh: các luật được thiết kế trước, nó sẽ quyết định gói tin nào được phép hoặc từ chối di chuyển qua nó

b) Lọc động: cho phép tường lửa phản ứng lại các sự kiện, hoặc tự tạo ra các luật để điều khiển các sự kiện đó

c) Kết hợp trạng thái: tường lửa theo dõi từng kết nối mạng giữa các hệ thống bên trong và bên ngoài bằng bảng trạng thái. Nó không những kiểm tra các đặc điểm của gói tin mà lưu giữ và kiểm tra trạng thái của các gói tin đi qua

3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

i. Tường lửa lọc gói tin

Ví dụ:

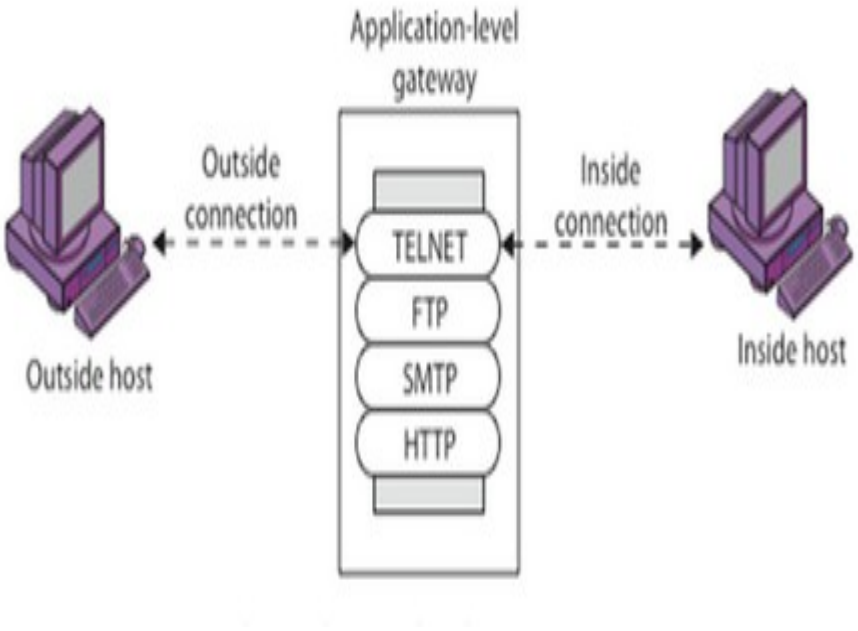
Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

ii. Application gateways (Tường lửa cổng ứng dụng)

Định nghĩa: còn được gọi là các máy chủ proxy, chúng có thể lọc gói ở lớp ứng dụng trong mô hình OSI. Các gói vào hoặc ra không thể truy cập các dịch vụ mà không có proxy.

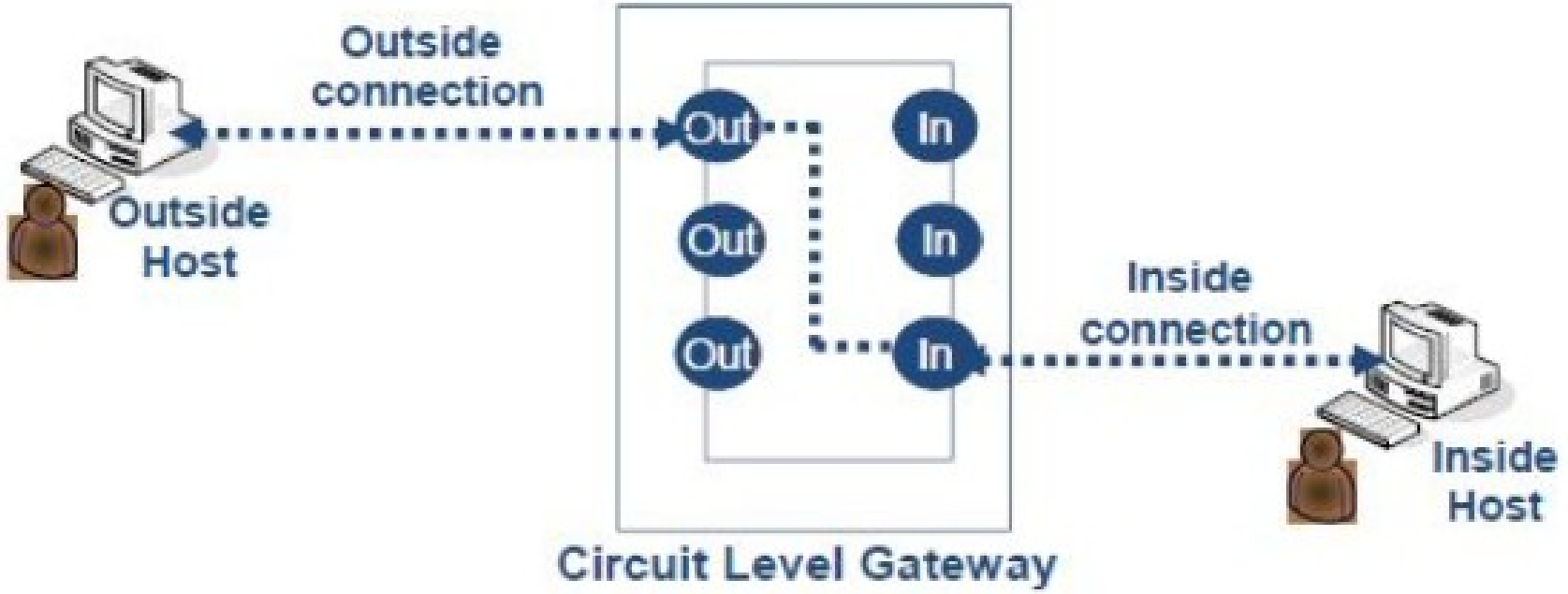


3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

iii. Circuit gateway firewall

- Thực thi ở tầng giao vận
- Nó không xem được luồng giữ liệu giữa 2 mạng
- Ngăn chặn kết nối trực tiếp giữa 2 mạng

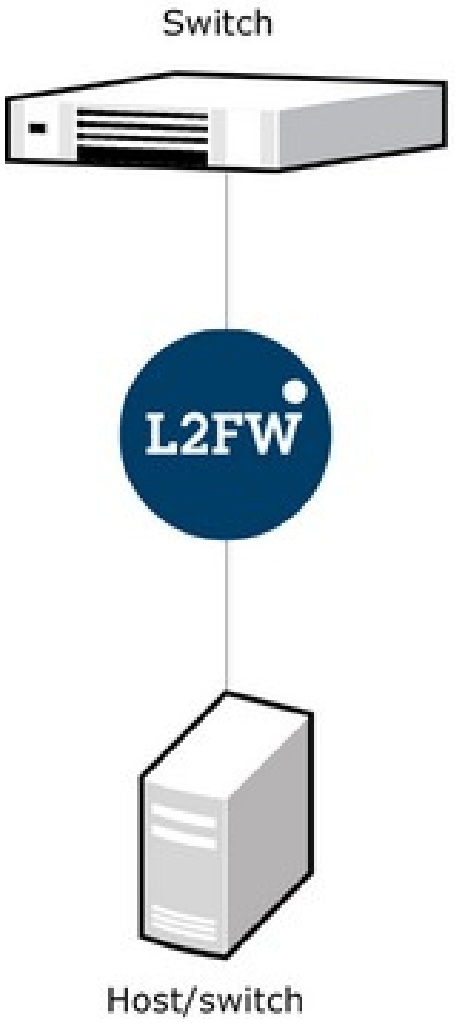


3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

iv. MAC layer firewalls

- Thực thi ở tầng liên kết
- Cho phép lọc theo một danh sách các chủ biết trước theo địa chỉ MAC

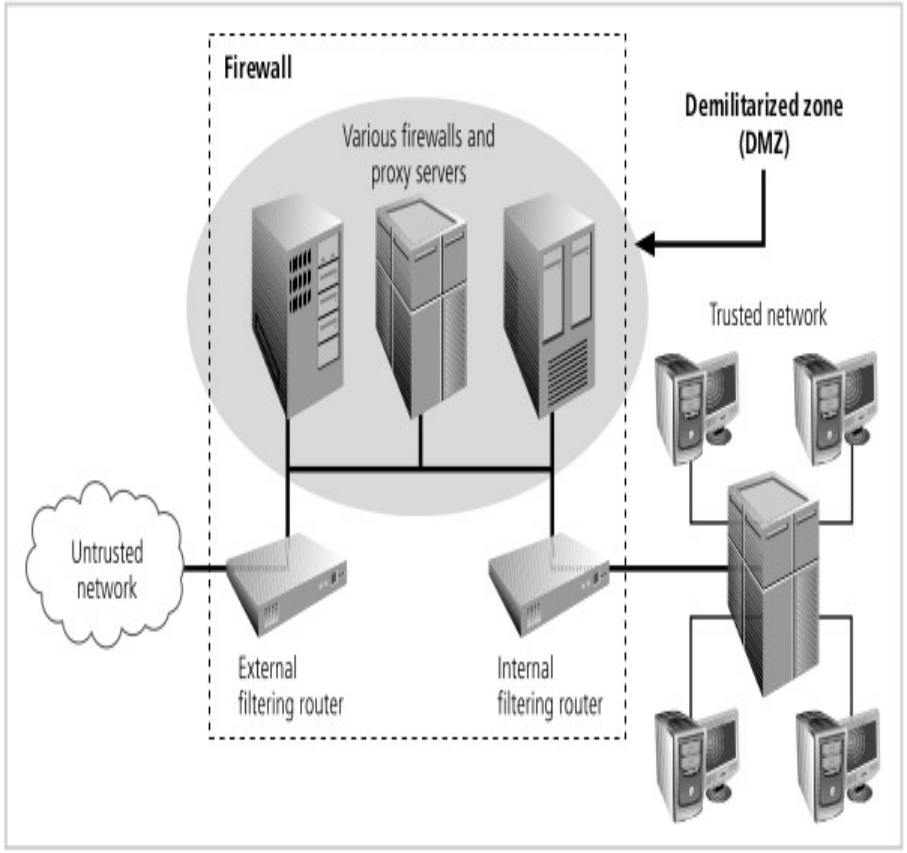


3. Bức tường lửa (firewall)

3.2. Phân loại bức tường lửa:

iv. Hybrid firewalls

- Là tường lửa kết hợp 4 loại ở trên như lọc gói, lọc MAC, lọc cổng, hoặc circuit gateways
- Hoặc kết hợp các loại tường lửa trên song song



3. Bức tường lửa (firewall)

3.3. Kiến trúc bức tường lửa

i. packet filtering router

ii. screened host firewalls

iii. dual-homed firewalls

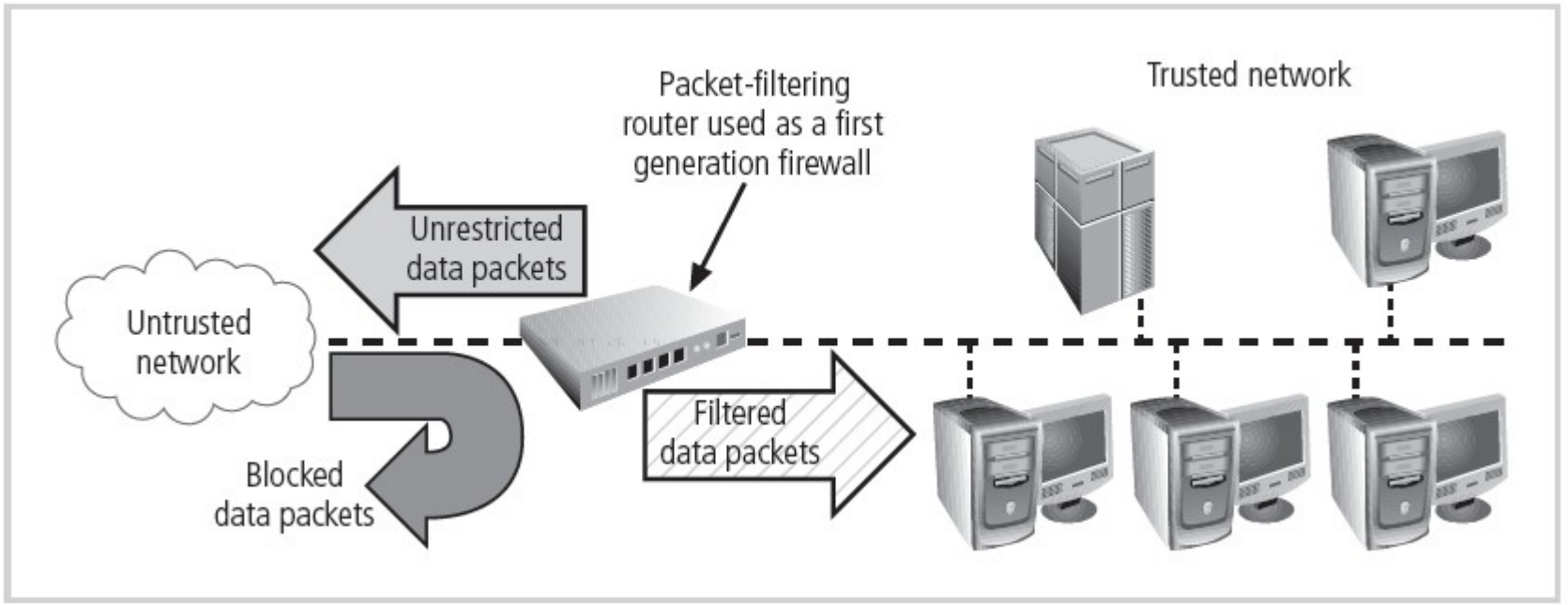
iv. screened subnet firewalls

3. Bức tường lửa (firewall)

3.3. Kiến trúc bức tường lửa

i. packet filtering router: xử dụng bộ định tuyến của router để cấu hình để từ chối các gói tin vào ra trong hệ thống

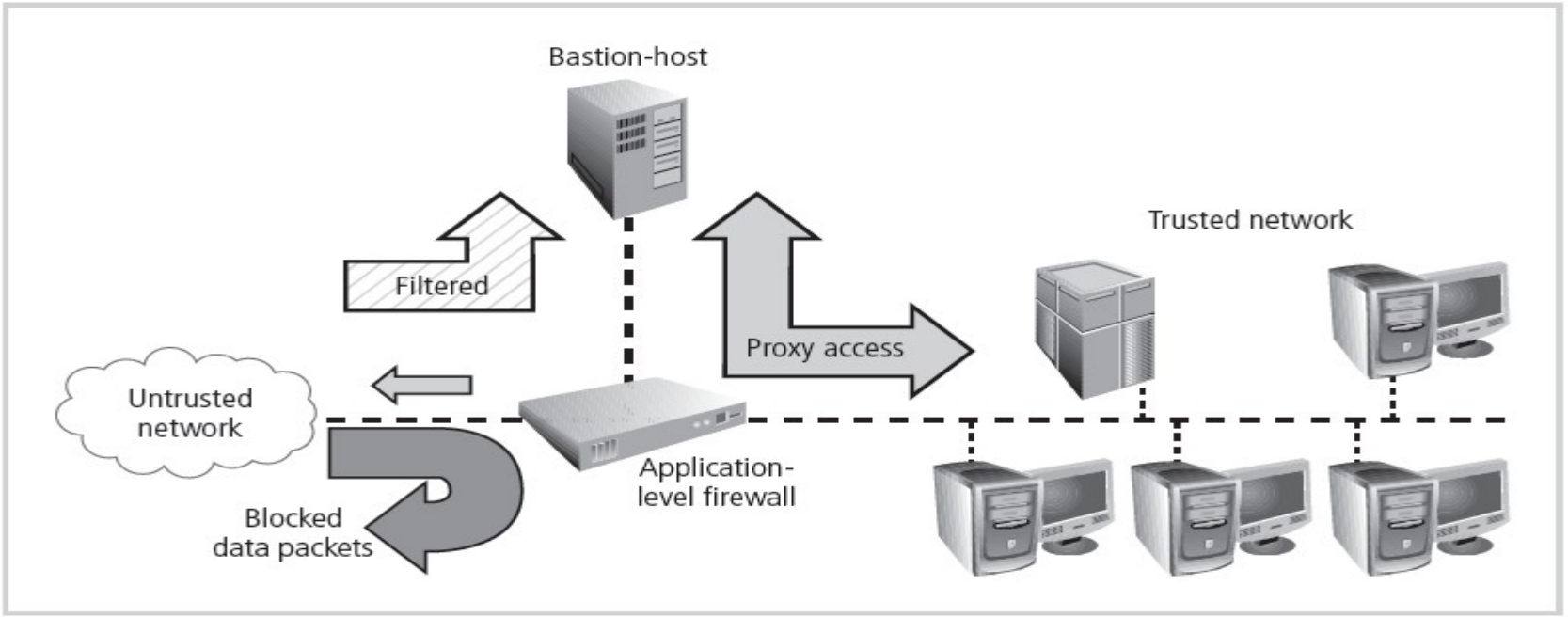
Hạn chế trong việc kiểm soát và xác thực tính hợp lệ



3. Bức tường lửa (firewall)

3.3. Kiến trúc bức tường lửa

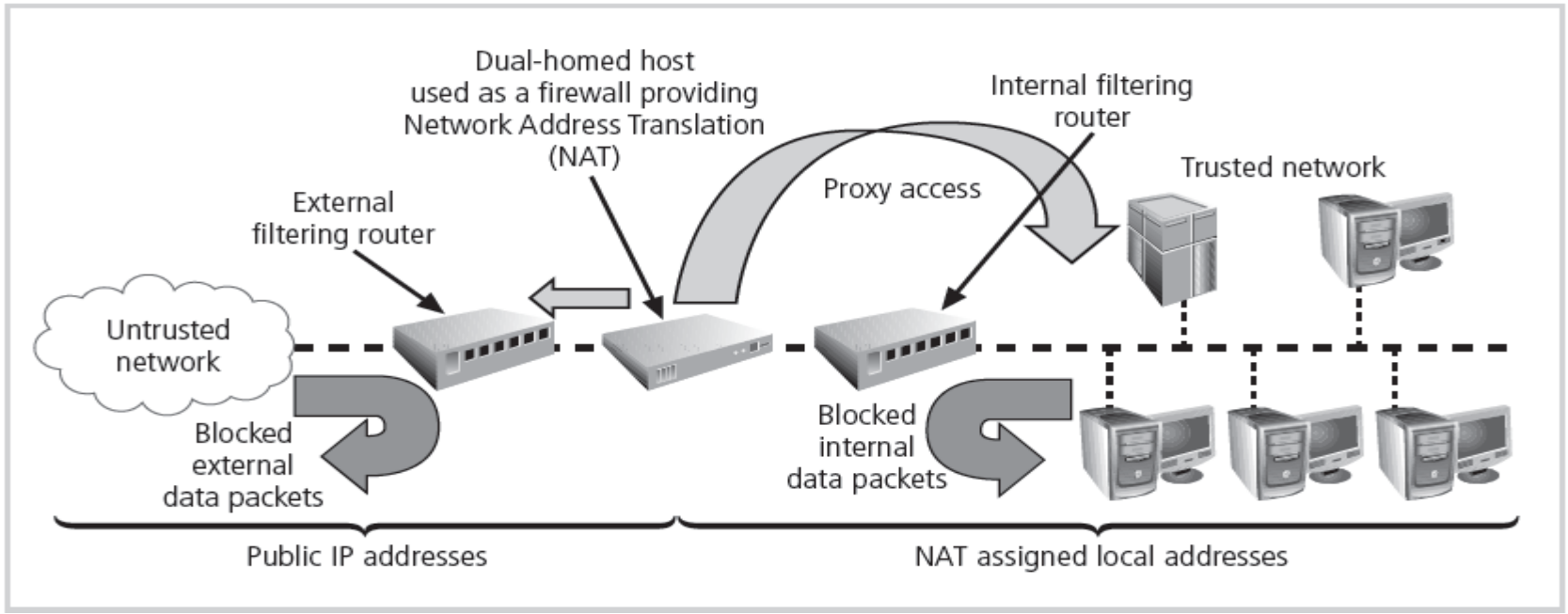
ii. screened host firewalls: kết hợp giữa lọc gói và các tường lửa chuyên biệt để nhìn trước các gói tin để giảm thiểu lưu lượng trong mạng nội bộ



3. Bức tường lửa (firewall)

3.3. Kiến trúc bức tường lửa

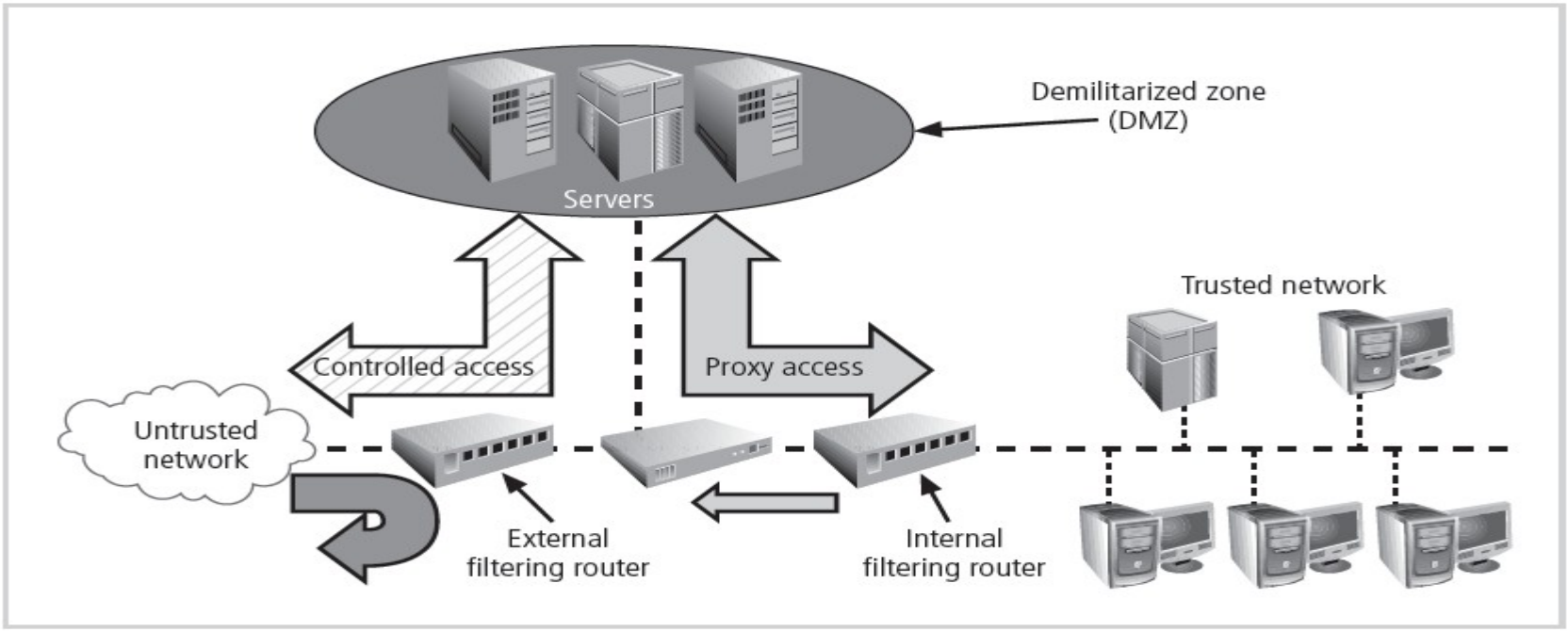
iii. dual-homed firewalls: là máy chủ pháo đài (bastion host) có 2 card mạng, 1 kết nối vào mạng nội bộ, 2 kết nối ra ngoài mạng. Nó dụng NAT để ánh xạ, và là 1 rào cản cho xác xâm nhập ngoài



3. Bức tường lửa (firewall)

3.3. Kiến trúc bức tường lửa

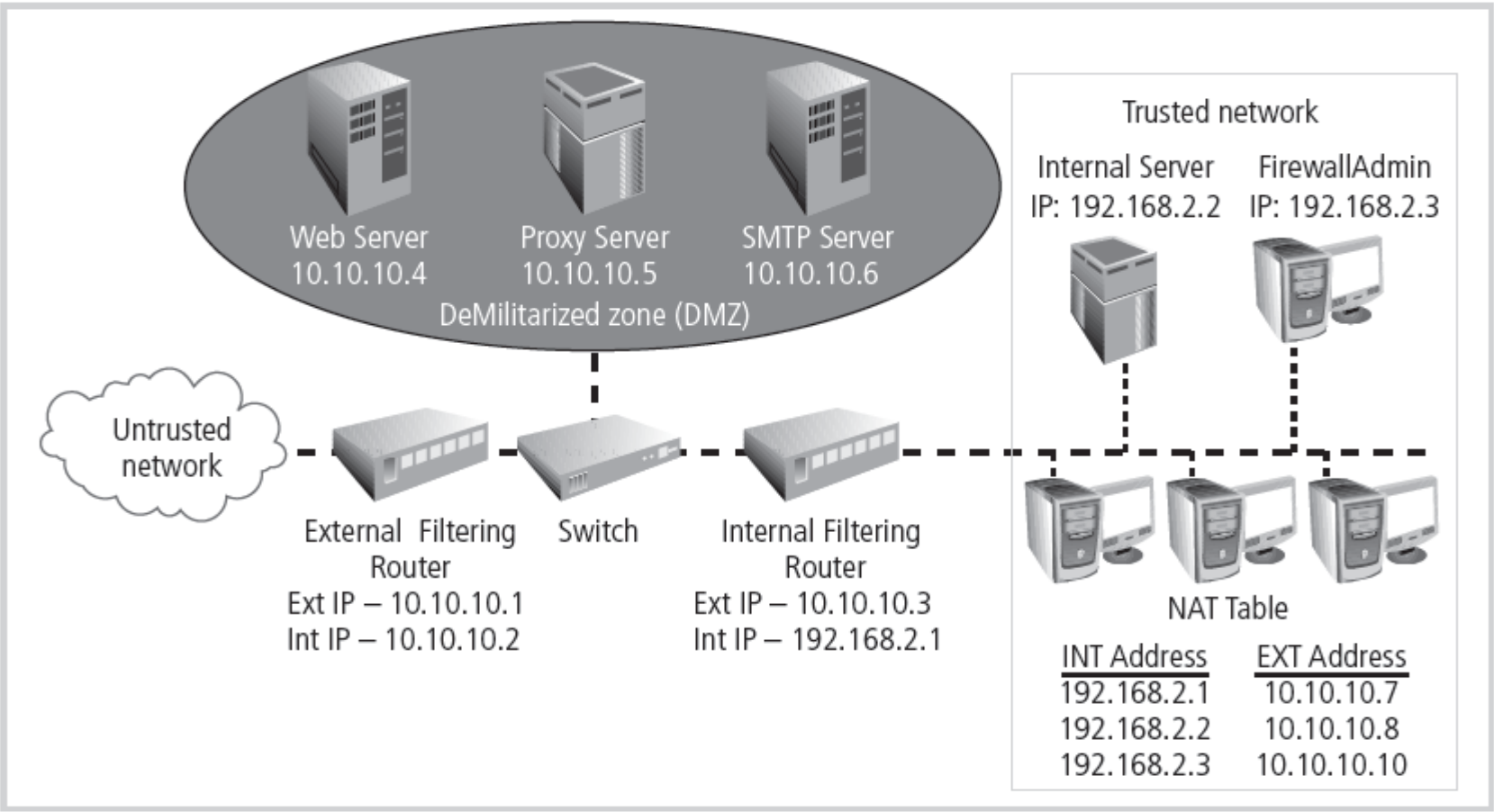
iv. screened subnet firewalls: bao gồm nhiều hơn 1 máy chủ pháo đài. Kết nối định tuyến ra mạng ngoài thông qua bộ định tuyến lọc ngoài, Kết nối tới mạng trong chỉ được kết nối từ khu vực DMZ thông qua bộ định tuyến lọc trong



3. Bức tường lửa (firewall)

3.4. Ví dụ cấu hình và quản lý bức tường lửa

Topo đồ mạng được thiết kế như sau



3. Bức tường lửa (firewall)

3.4. Ví dụ cấu hình và quản lý bức tường lửa

Một số cổng phổ biến

Port Number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

3. Bức tường lửa (firewall)

3.4. Ví dụ vấu hình và quản lý bức tường lửa

Một số bộ luật được cấu hình cho tường lửa mạng trong

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	10.10.10.0	Any	Any	Any	Deny
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	Any	Any	10.10.10.0	>1023	Allow
7	Any	Any	10.10.10.6	25	Allow
8	Any	Any	10.10.10.0	7	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.4	80	Allow
11	Any	Any	Any	Any	Deny

3. Bức tường lửa (firewall)

3.4. Ví dụ vấu hình và quản lý bức tường lửa

Một số bộ luật được cấu hình cho bộ lọc tường lửa mạng ngoài

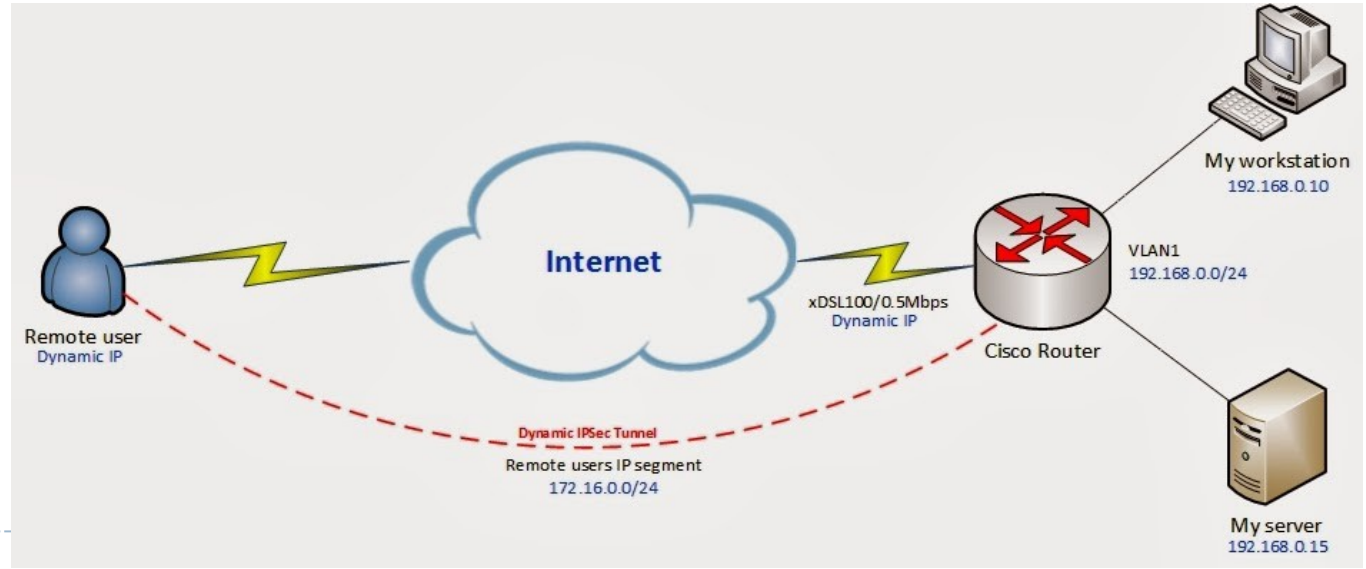
Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	10.10.10.12	Any	10.10.10.0	Any	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	10.10.10.0	Any	Any	Any	Allow
7	Any	Any	Any	Any	Deny

4. Truy cập từ xa và VPNs

i. Truy cập từ xa: Việc truy cập từ xa vào một hệ thống yêu cầu phải thông qua một kênh truyền tin cậy, sử dụng các giao thức bảo mật.

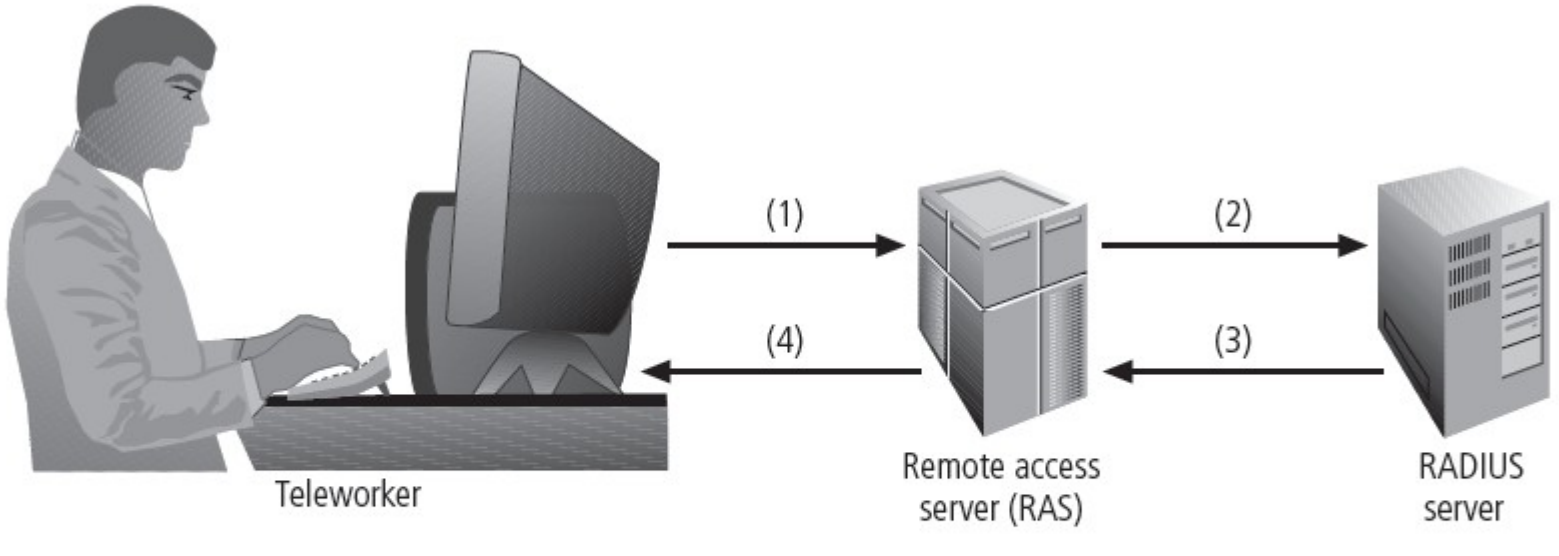
- Mạng riêng ảo (VPNs) là một kênh truyền tin cậy được lựa chọn

- Cơ chế xác thực được sử dụng là – RADIUS, TACACS; CHAP



4. Truy cập từ xa và VPNs

i.Truy cập từ xa: RADIUS là 1 server để xử lý việc xác thực của người dùng chung trong toàn bộ hệ thống

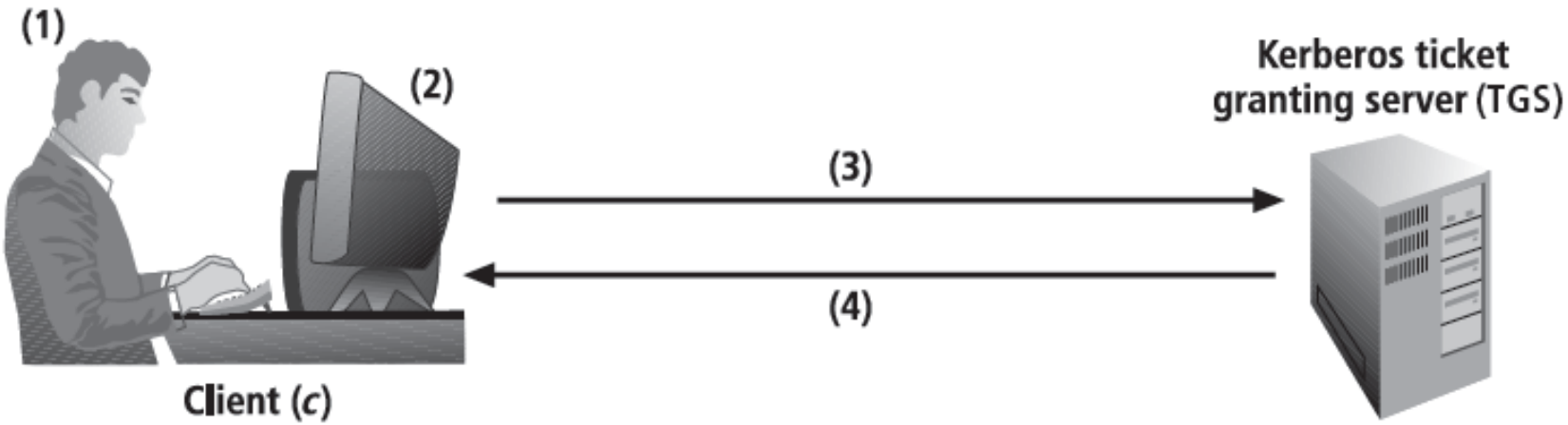


1. Remote worker dials RAS and submits username and password
2. RAS passes username and password to RADIUS server
3. RADIUS server approves or rejects request and provides access authorization
4. RAS provides access to authorized remote worker

4. Truy cập từ xa và VPNs

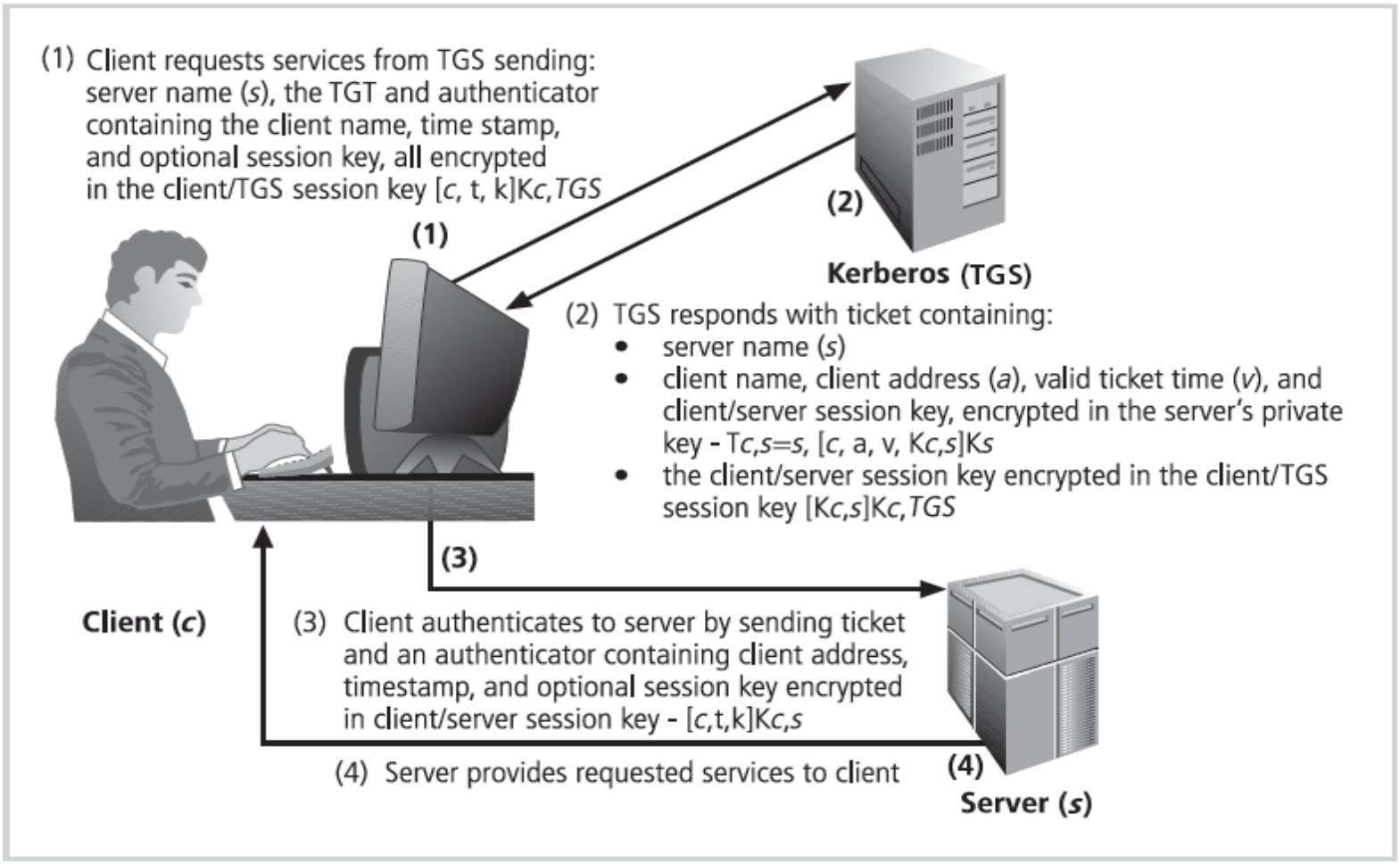
i.Truy cập từ xa: Mô hình đăng nhập của Kerberos

(1) User logs into client machine (*c*)
(2) Client machine encrypts password to create client key (K*c*)
(3) Client machine sends clear request to Kerberos TGS
(4) Kerberos TGS returns ticket consisting of:
- Client/TGS session key for future communications between client and TGS [K*c*,TGS], encrypted with the client's key
- Ticket granting ticket (TGT). The TGT contains the client name, client address, ticket valid times, and the client/TGS session key, all encrypted in the TGS' private key



4. Truy cập từ xa và VPNs

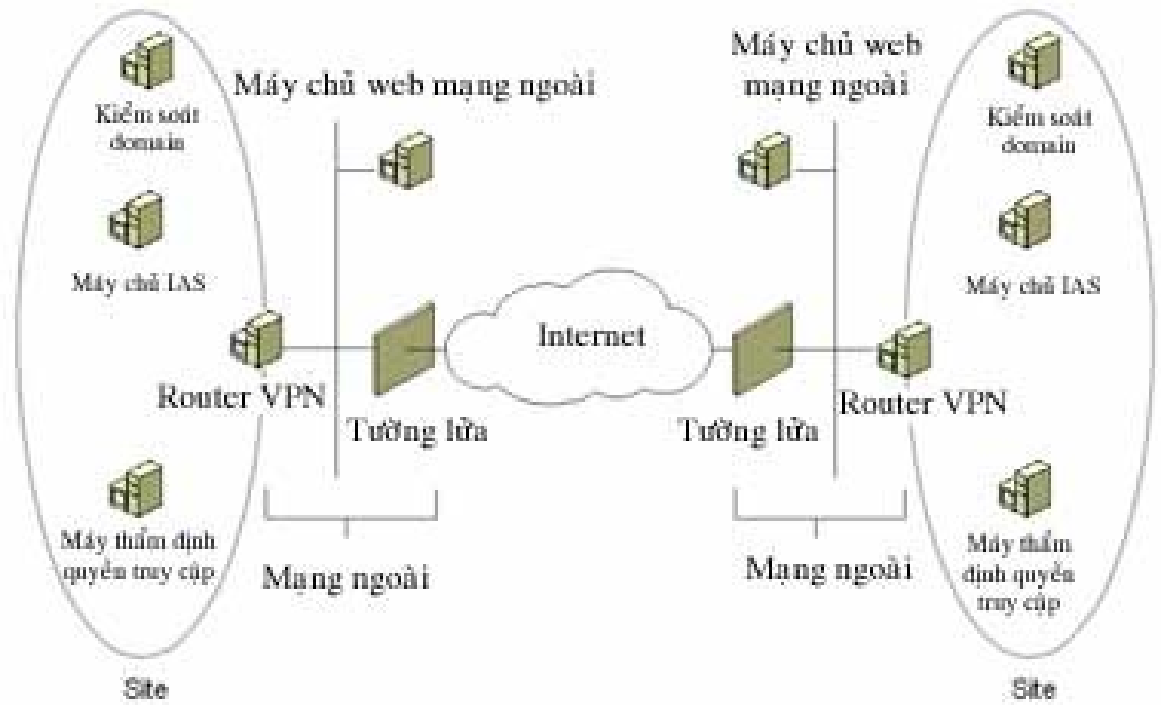
i.Truy cập từ xa: yêu cầu các dịch vụ của Kerberos



4. Truy cập từ xa và VPNs

ii.VPNs - là mạng riêng ảo cho phép tạo ra những kết nối tới liên kết mạng khác một cách an toàn thông qua Internet.

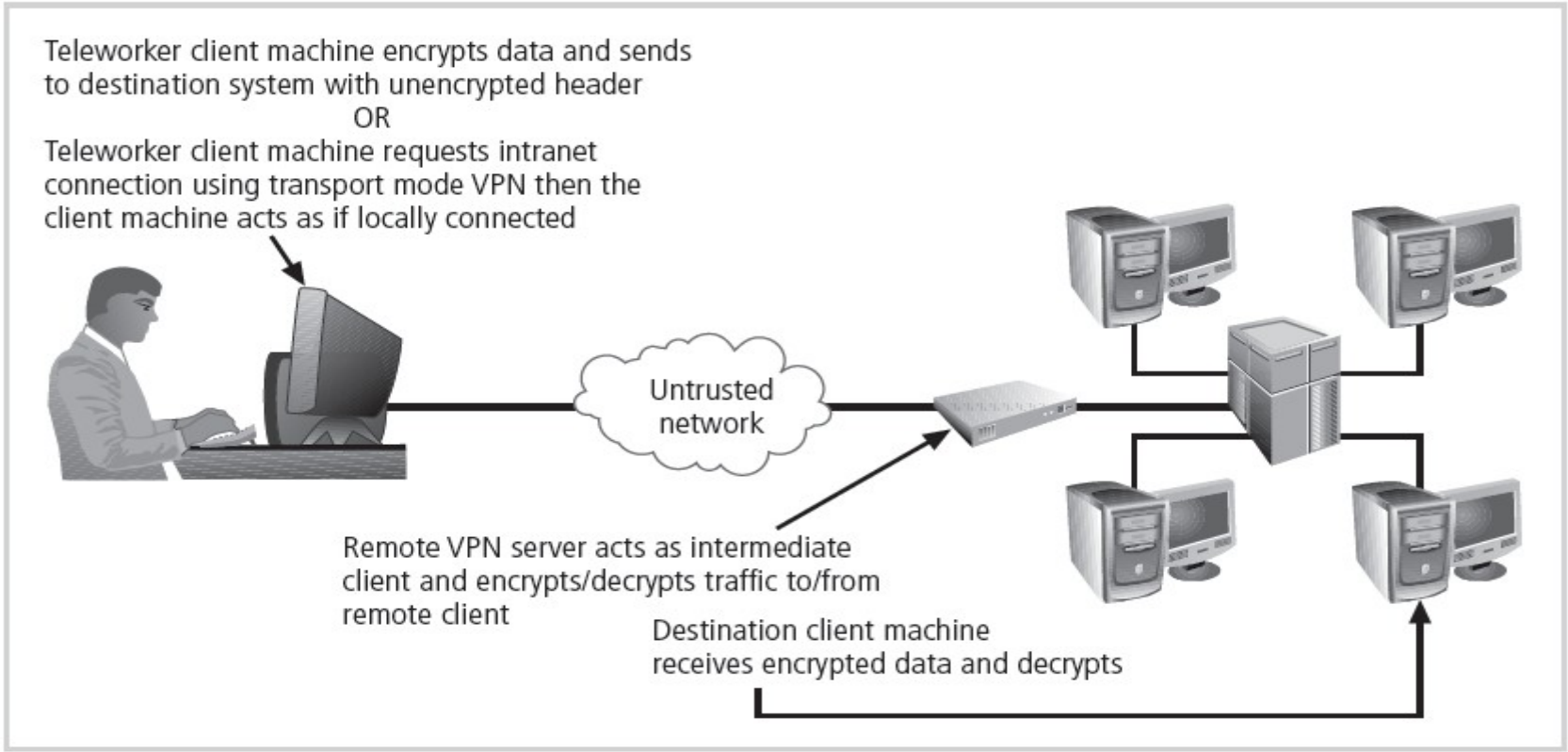
- Mở rộng an toàn các kết nối mạng nội bộ của tổ chức đến các địa điểm từ xa ngoài mạng đáng tin cậy



4. Truy cập từ xa và VPNs

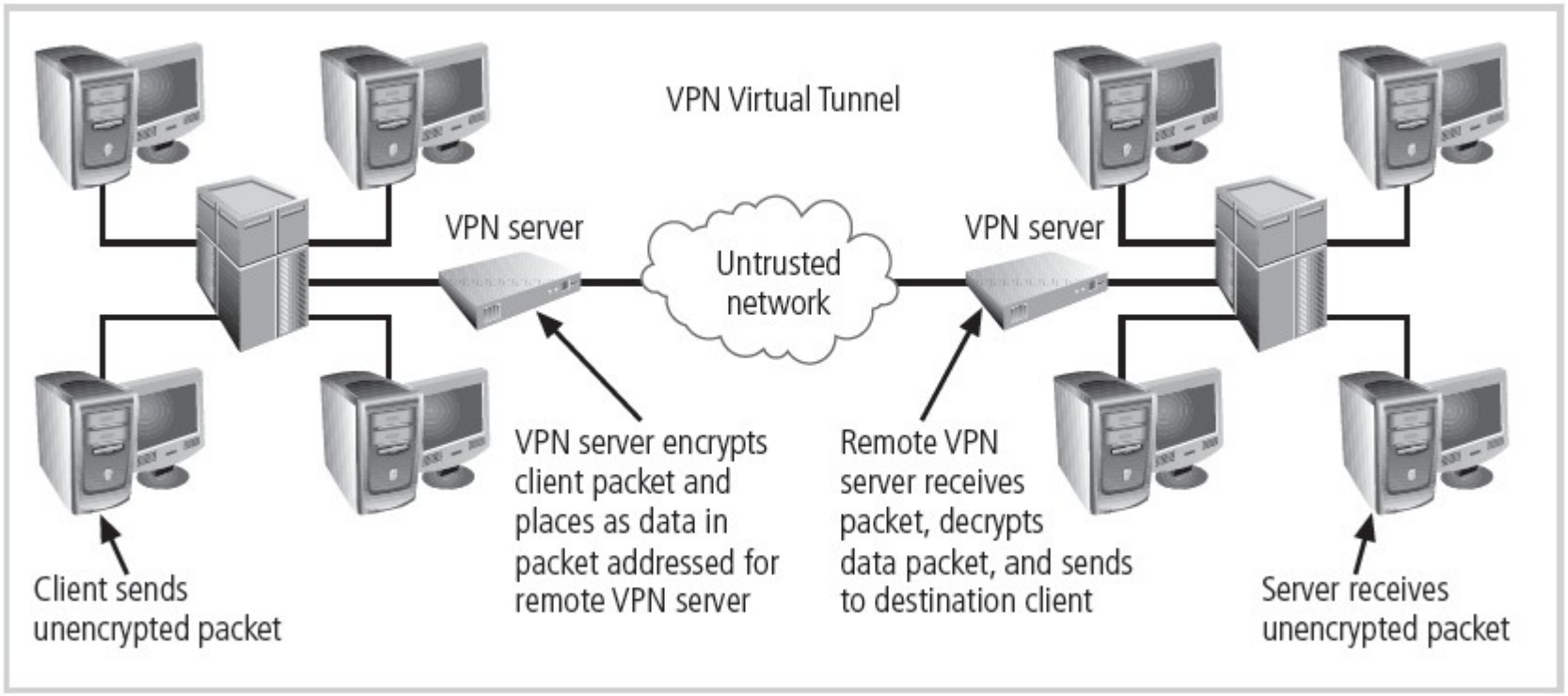
ii.VPNs - Làm việc trên tầng giao vận

- Dữ liệu gói tin được mã hóa, nhưng thông tin header thì không mã hóa



4. Truy cập từ xa và VPNs

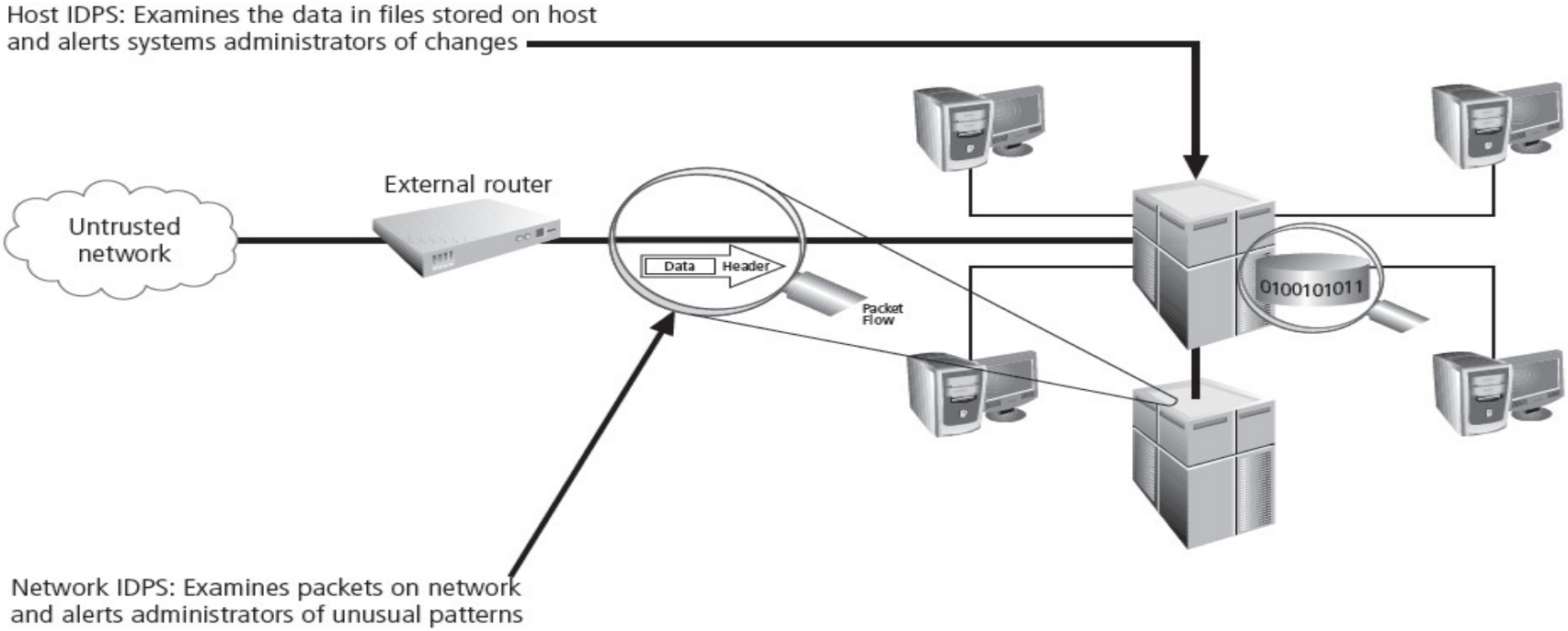
ii.VPNs - Chế độ đường hầm - Các máy chủ hoạt động như các điểm mã hóa, mã hóa tất cả gói tin đi qua nó



5. IDSs và IPSs

i.Định nghia - là hệ thống phát hiện và ngăn chặn xâm nhập mạng

ii.Phân loại - host-base IDSs và network-base IDSs



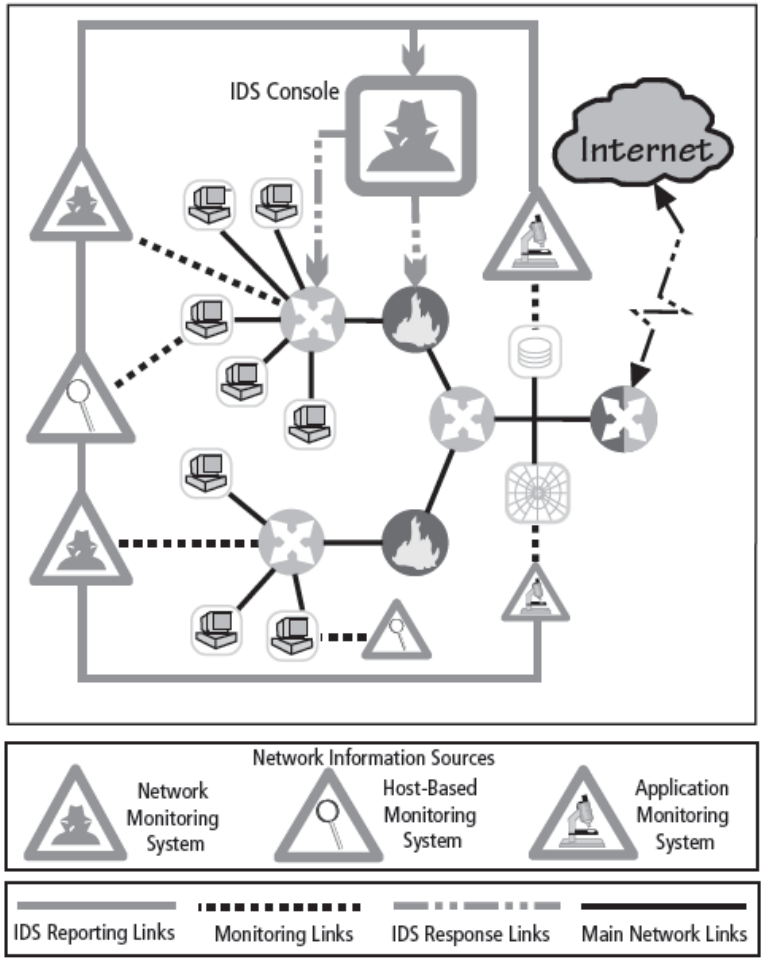
5. IDSs và IPSs

iii. Phương pháp phát hiện

a. So khớp tập mẫu - so khớp dữ liệu thu được với tập mẫu để tìm ra bất thường

b. Thống kê - thống kê các hành vi của mạng để tìm ra các bất thường

c. Kết hợp cả 2 phương pháp trên

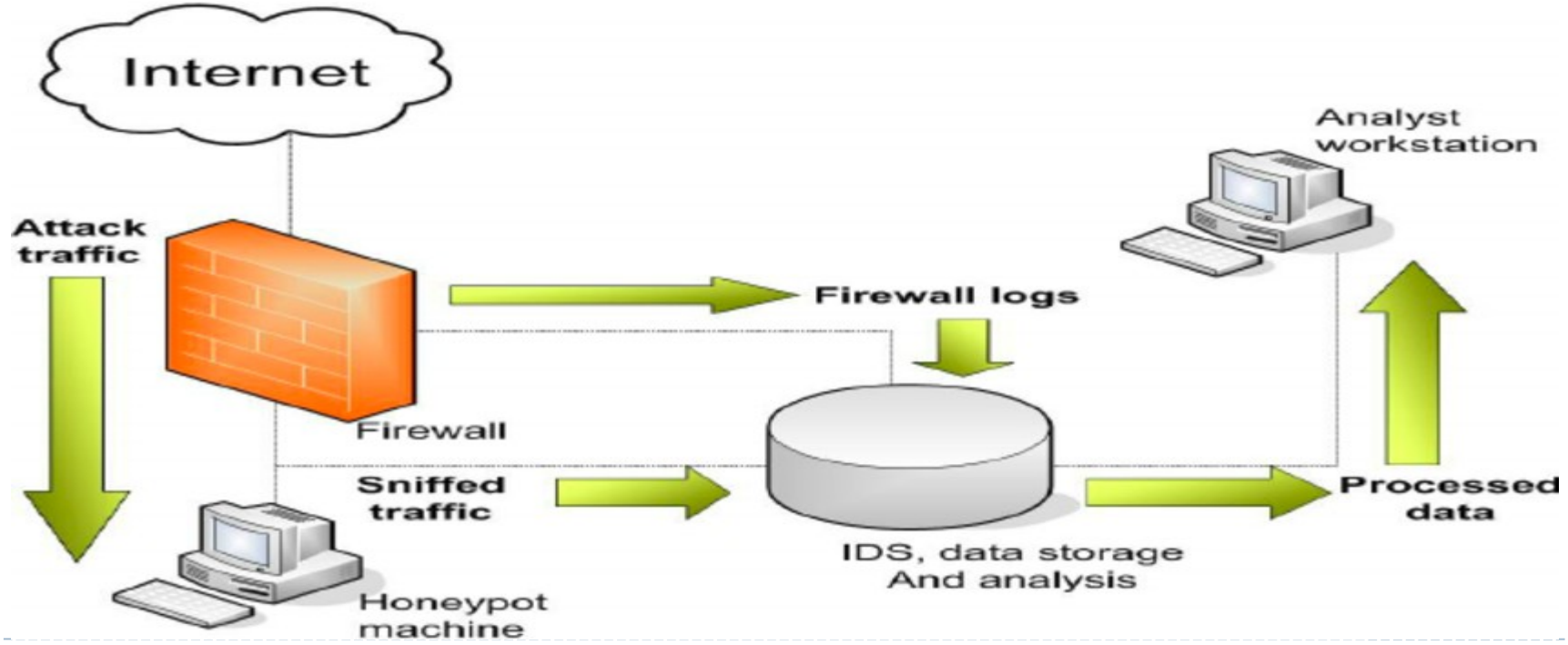


5. IDSs và IPSs

iv. honeypots, honeynets

a. honeypots - hệ thống mồi được thiết kế để thu hút những kẻ tấn công

b. honeynets - mạng các honeypots kết nối một số hệ thống



5. IDSs và IPSs

v. Một số công cụ

a. Công cụ giám sát hệ thống - htop, system mamager..

b. Công cụ quét - nmap, metasploit, ping ..

c. Công cụ tường lửa - phần mần mềm, thiết bị phần cứng trên window, ubuntu..

d. Công cụ quét lỗ hổng - openvas, nessus..

e. Công cụ chặn bắt gói tin - wireshark, tshark, tcpdump..

6. BÀI TẬP - THẢO LUẬN

1.How is an application layer firewall different from a packet-filtering firewall? Why is an application layer firewall sometimes called a proxy server?

2.What is a hybrid firewall?

3.What a sacrificial host? What is a bastion host?

4.What is a DMZ?

5.What is RADIUS?

6.What is a honeypot? How is it different from a honeynet?

HỎI VÀ ĐÁP