Mật mã và An ninh mạng

Chương 7:

An toàn mạng máy tính

Chương 7. An toàn mạng máy tính

7.1 Giới thiệu về an toàn mạng máy tính

7.2 Bức tường lửa (Firewall)

7.3 Mạng riêng ảo VPN

7.4 VLAN

7.5 NAT

7.1 Giới thiệu về an toàn mạng máy tính

1. Các nguyên tắc nền tảng của an ninh mạng

An ninh mạng máy tính (network security) là tổng thể các giải pháp về mặt tổ chức và kỹ thuật nhằm ngăn cản mọi nguy cơ tổn hại đến mạng.

1. Các nguyên tắc nền tảng của an ninh mạng

Các tổn hại có thể xảy ra do:

- Lỗi của người sử dụng,
- Các lỗ hổng trong các hệ điều hành cũng như các chương trình ứng dụng,
- Các hành động hiểm độc,
- Các lỗi phần cứng,
- Các nguyên nhân khác từ tự nhiên.

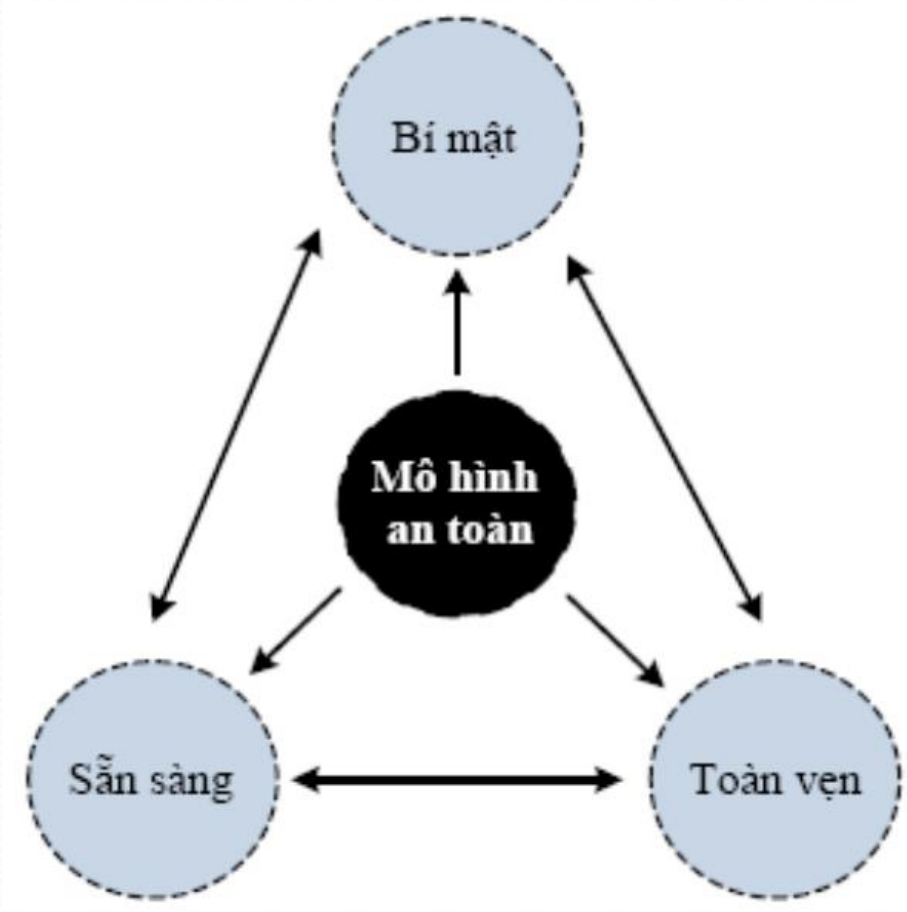
1. Các nguyên tắc nền tảng của an ninh mạng

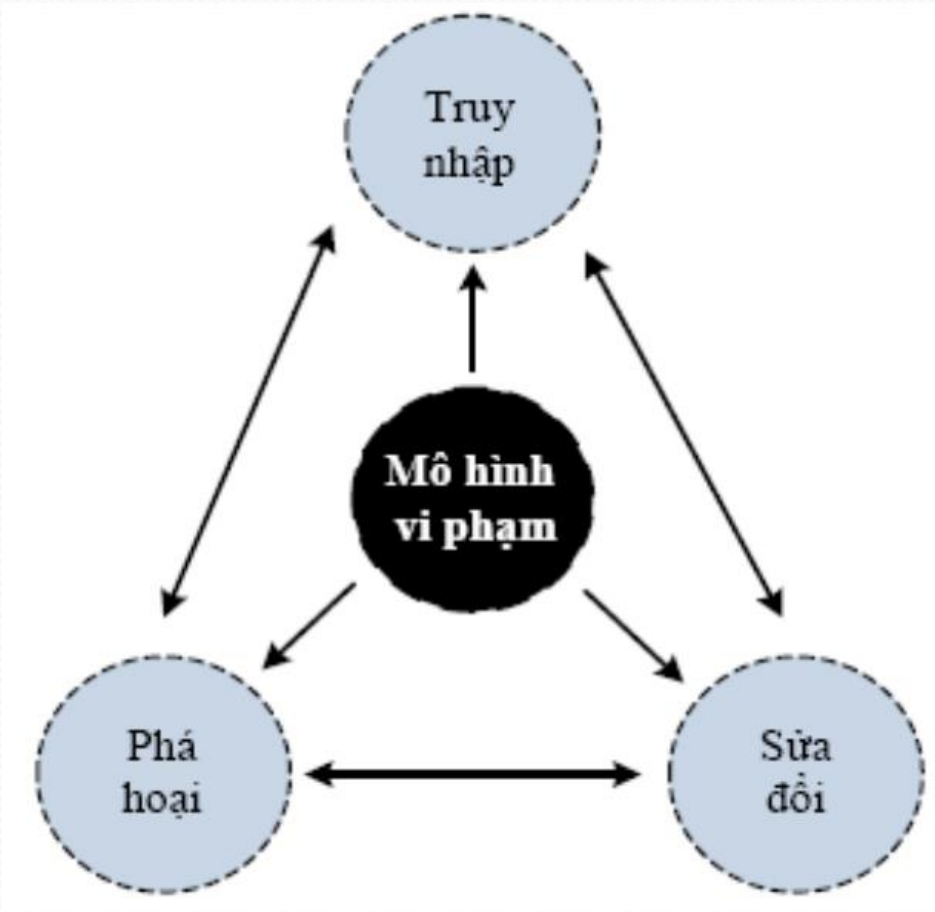
Mô hình CIA

- Confidentiality: Tính bí mật.
- Integrity: Tính toàn vẹn.
- Availability: Tính sẵn sàng.

1. Các nguyên tắc nền tảng của an ninh mạng

Mô hình CIA (Confidentiality, Integrity, Availability)





Mô hình CIA

a) Tính bí mật

- Sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm.
- Khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhạy cảm đó được che giấu với người dùng không được cấp phép

Mô hình CIA

b) Tính toàn vẹn

Sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó đảm bảo được sự chính xác của thông tin và hệ thống.

Mô hình CIA

b) Tính toàn vẹn

Mục đích chính:

- Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.
- Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chủ tâm của những người sử dụng được phép.
- Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

Mô hình CIA

c) Tính sẵn sàng

Bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và tới mạng.

Mô hình CIA

c) Tính sẵn sàng có liên quan đến độ tin cậy của hệ thống.

Mô hình DAD

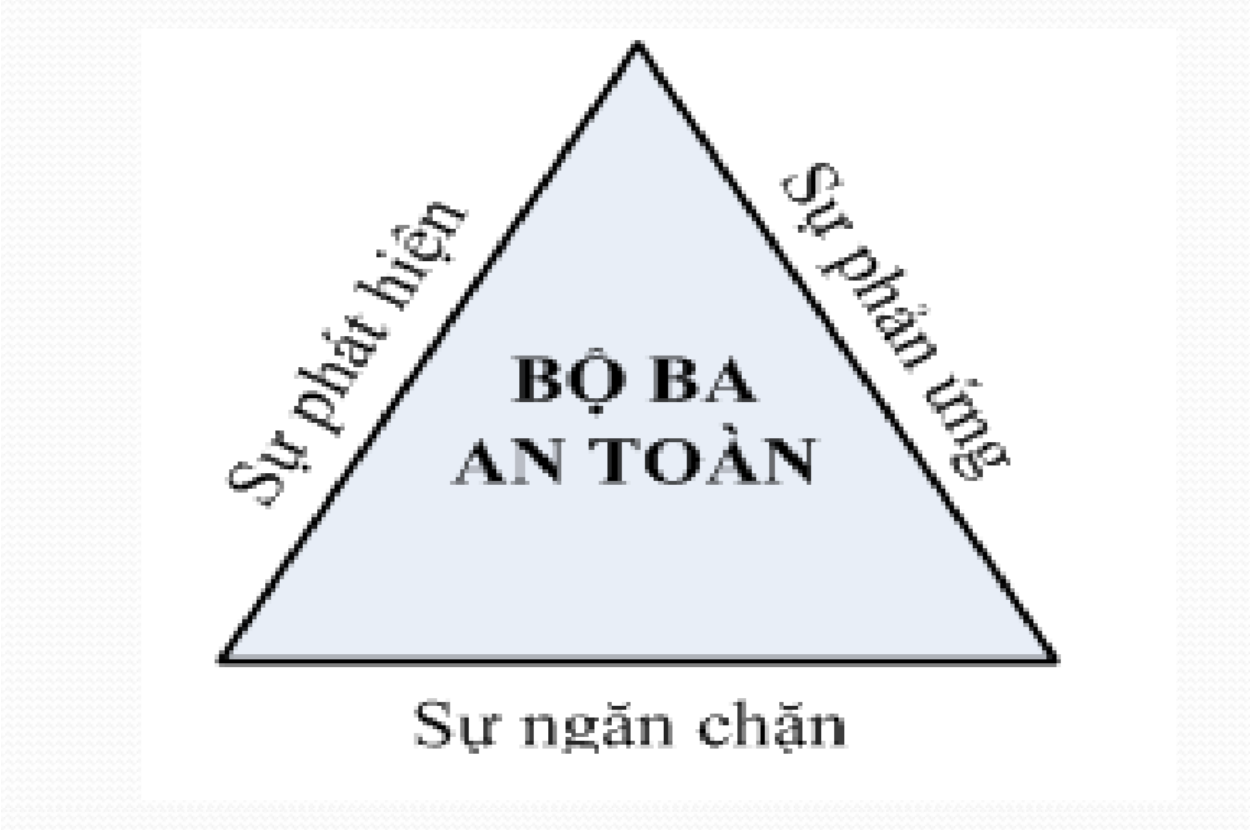
- Sự truy nhập (Disclosure): chống lại tính bí mật.
- Sự sửa đổi (Alteration): chống lại tính toàn vẹn.
- Sự phá hoại (Destruction): chống lại tính sẵn sàng

d) Các chức năng khác

- Sự định danh (Identification): hành động của người sử dụng khi xác nhận một sự định danh tới hệ thống, ví dụ định danh thông qua tên (username) của cá nhân.
- Sự xác thực (Authentication): sự xác minh rằng định danh đã khai báo của người sử dụng là hợp lệ, ví dụ thông qua việc sử dụng một mật khẩu (password).
- Sự kiểm toán (Accountability): sự xác định các hành động hoặc hành vi của một cá nhân bên trong hệ thống và nắm chắc được trách nhiệm cá nhân hoặc các hành động của họ.
- Sự ủy quyền (Authorization): các quyền được cấp cho một cá nhân (hoặc tiến trình) mà chúng cho phép truy cập vào tài nguyên trên mạng hoặc máy tính.
- Sự chống chối từ (Non-repudiation): bảo đảm không có khả năng chối bỏ hành động đã thực hiện ở người gửi và người nhận

2. Mô hình bộ ba an ninh

- Sự phát hiện (Detection)
- Sự ngăn chặn (Prevention)
- Sự phản ứng (Response)



a) Sự ngăn chặn (Prevention)

- Là nền tảng của bộ ba an ninh
- Cung cấp mức độ an ninh cần thiết nào đó để thực hiện các biện pháp ngăn chặn sự khai thác các lỗ hổng.
- Cần phải nhấn mạnh vào các biện pháp ngăn chặn hơn là vào sự phát hiện và sự phản ứng vì sẽ là dễ dàng, hiệu quả và có giá trị nhiều hơn để ngăn chặn một sự vi phạm an ninh hơn là thực hiện phát hiện hoặc phản ứng với nó.

b) Sự phát hiện (Detection)

- Cần có các biện pháp cần thiết để thực hiện phát hiện các nguy cơ hoặc sự vi phạm an ninh trong trương hợp các biện pháp ngăn chặn không thành công.
- Một sự vi phạm được phát hiện sớm sẽ dễ dàng hơn để làm mất tác hại và khắc phục nó. Như vậy, sự phát hiện không chỉ được đánh giá về mặt khả năng, mà còn về mặt tốc độ, tức là phát hiện phải nhanh

c) Sự phản ứng (Response)

- Phải phát triển một kế hoạch để đưa ra phản ứng phù hợp đối với một số lỗ hổng an ninh.
- Kế hoạch phải được viết thành văn bản và phải xác định ai là người chịu trách nhiệm cho các hành động nào và khi thay đổi các phản ứng và các mức độ cần tăng cường.
- Tính năng phản ứng của một hệ thống an ninh không chỉ là năng lực, mà còn là vấn đề tốc độ.

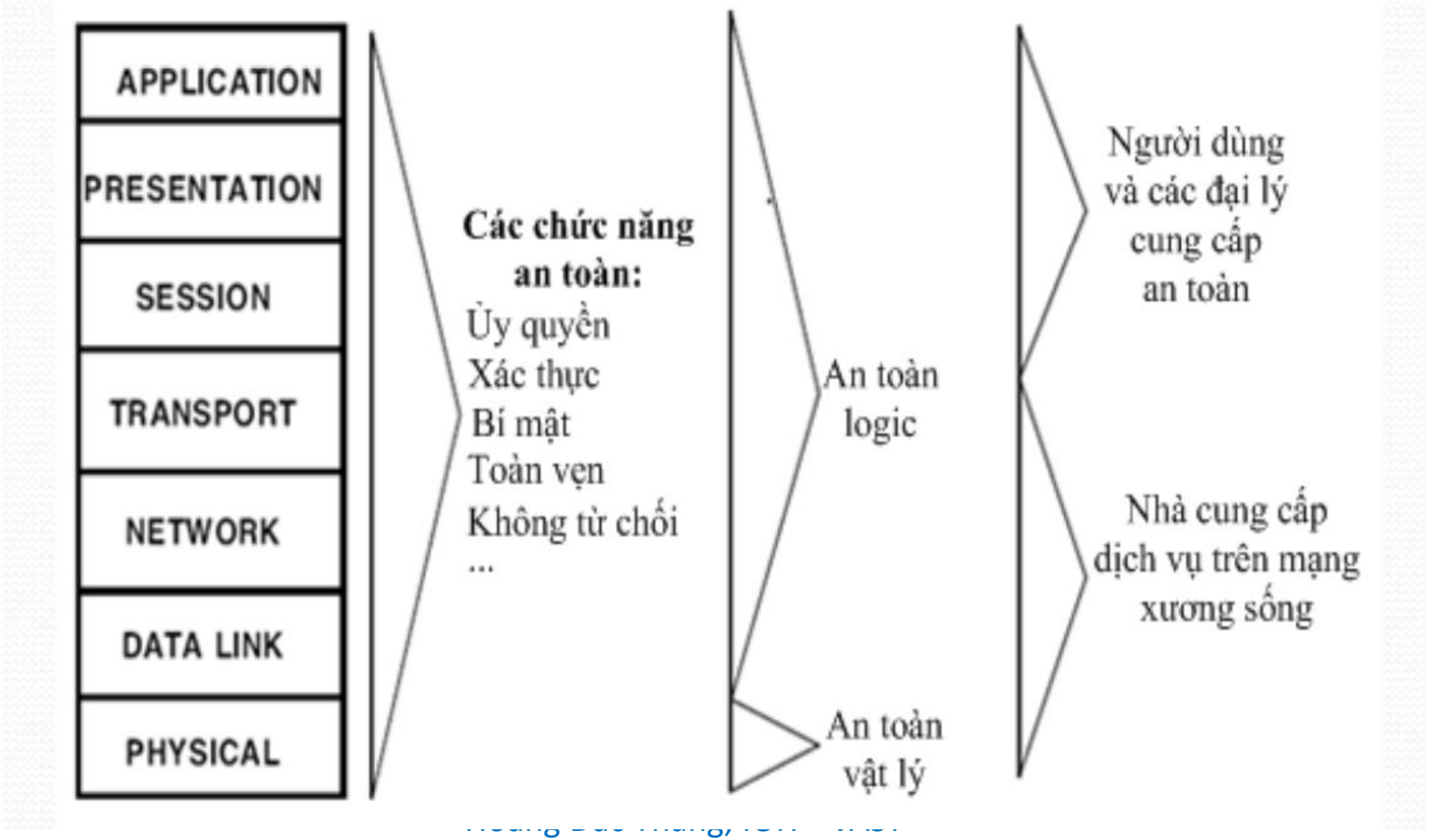
2. Mô hình bộ ba an ninh

Ngày nay các cuộc tấn công mạng rất đa dạng, sẽ không thể đoán chắc được chúng sẽ xảy ra khi nào, ở đâu, dạng nào và hậu quả của chúng.

Để đảm bảo an ninh cho một mạng thì cần:

- Phát hiện nhanh,
- Phản ứng nhanh
- Ngăn chặn thành công mọi hình thức tấn công.

3. An ninh mạng và OSI



7.2 Bức tường lửa (Firwall)

1. Bức tường lửa là gì?

- Cửa khẩu để kiểm soát và theo dõi. Luồng thông tin chỉ được qua cửa duy nhất này.
- Một hệ thống gồm phần cứng và/hoặc phần mềm có chức năng chặn và lọc giao thông dữ liệu giữa hệ thống bên trong và môi trường bên ngoài.
- Giữ những điều xấu không thể lan vào bên trong hệ thống. Firwall được cài đặt các chính sách an toàn, thiết kế cụ thể để tránh những điều xấu cụ thể có thể xảy ra.

1. Bức tường lửa là gì?

Hạn chế của bức tường lửa

- Không bảo vệ được các tấn công đi vòng qua nó, chẳng hạn mạng lén lút, thiết bị modems.
- Ngăn cản cả các tổ chức tin cậy và dịch vụ tin cậy (SSL/SSH).
- Không bảo vệ chống các mối đe dọa từ bên trong, chẳng hạn như những nhân viên bực tức hoặc thông đồng với kẻ xấu.
- Không thể bảo vệ chống việc truyền các chương trình hoặc file nhiễm virus, vì có phạm vi rất rộng các dạng file và các hệ điều hành.

1. Bức tường lửa là gì?

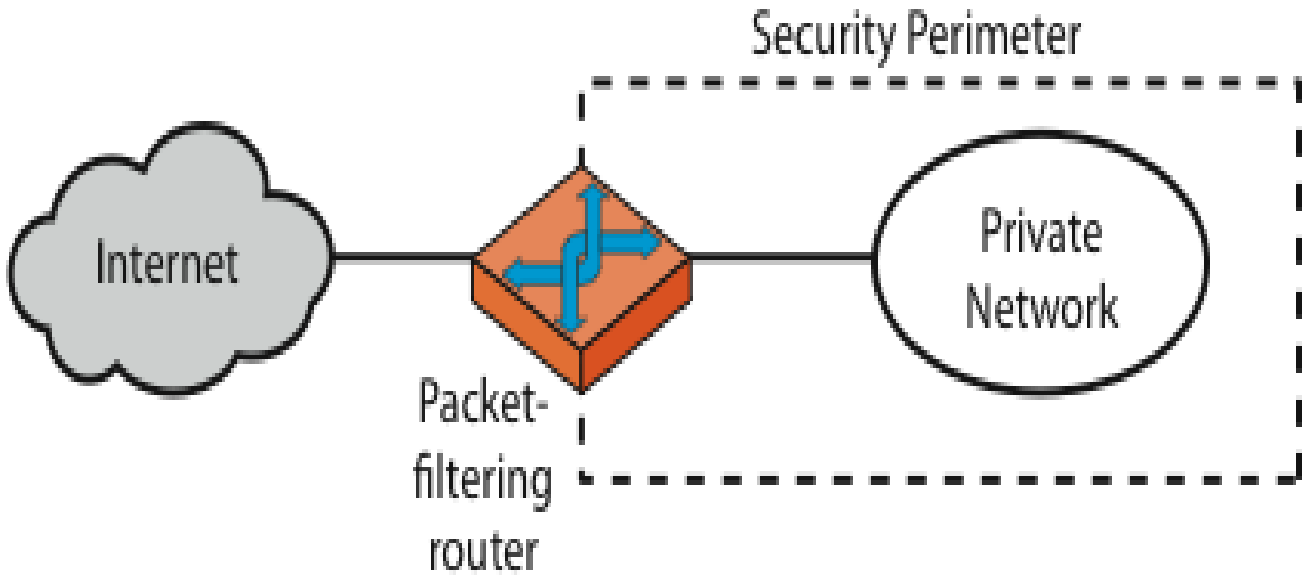
Một số loại bức tường lửa cơ bản:

- Cửa khẩu lọc gói (Packet Filtering Gateway)
- Tường lửa lọc gói trạng thái (Statefull Firewall)
- Cổng ứng dụng (Application-level gateway hay Application Proxy)
- Cổng giao tiếp mức mạch vòng (Circuite-level Gateway)

2. Cửa khẩu lọc gói (Packet Filtering Gateway)

- Là thành phần của bức tường lửa nhanh nhất và đơn giản nhất, là cơ sở của mọi hệ thống tường lửa.
- Nó kiểm tra mỗi gói IP (không có ngữ cảnh) và cho phép hay từ chối tuỳ theo qui tắc xác định. Suy ra có hạn chế truy cập đến các dịch vụ và các cổng.

2. Cửa khẩu lọc gói (Packet Filtering Gateway)



(a) Packet-filtering router

2. Cửa khẩu lọc gói (Packet Filtering Gateway)

Các chính sách mặc định có thể:

- Cái gì không bị nêu rõ ràng là cấm thì có nghĩa là được phép (NSD thích)
- Cái gì không nêu rõ ràng là được phép thì có nghĩa bị cấm (quản trị thích)

2. Cửa khẩu lọc gói (Packet Filtering Gateway)

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

2. Cửa khẩu lọc gói (Packet Filtering Gateway)

Tấn công các lọc gói

- Địa chỉ IP lừa đảo: giả địa chỉ nguồn làm cho tin tưởng, bổ sung bộ lọc lên mạch chuyển để ngăn chặn.
- Tấn công mạch truyền gốc: kẻ tấn công đặt được truyền khác với mặc định, ngăn chặn các gói truyền gốc
- Tấn công các đoạn tin (fragment) nhỏ. Chia thông tin phần đầu thành một số đoạn nhỏ. Hoặc bỏ qua hoặc sắp xếp lại trước khi kiểm tra

3. Tường lửa lọc gói trạng thái (Statefull Firewall)

- Lọc gói truyền thống không kiểm tra ngữ cảnh của tầng cao hơn, tức là so sánh các gói về với dòng chảy ra. Lọc gói trạng thái xét đến trạng thái của gói tin.
- Chúng kiểm tra mỗi gói IP trong ngữ cảnh: giữ vết theo dõi với các kỳ client-server, kiểm tra từng gói đúng thuộc vào một phiên.
- Chúng có khả năng tốt hơn phát hiện các gói giả tách khỏi ngữ cảnh.

4. Cổng ứng dụng

Cổng giao tiếp chuyên dùng cho ứng dụng – proxy (người được uỷ quyền). Truy cập đầy đủ đến giao thức:

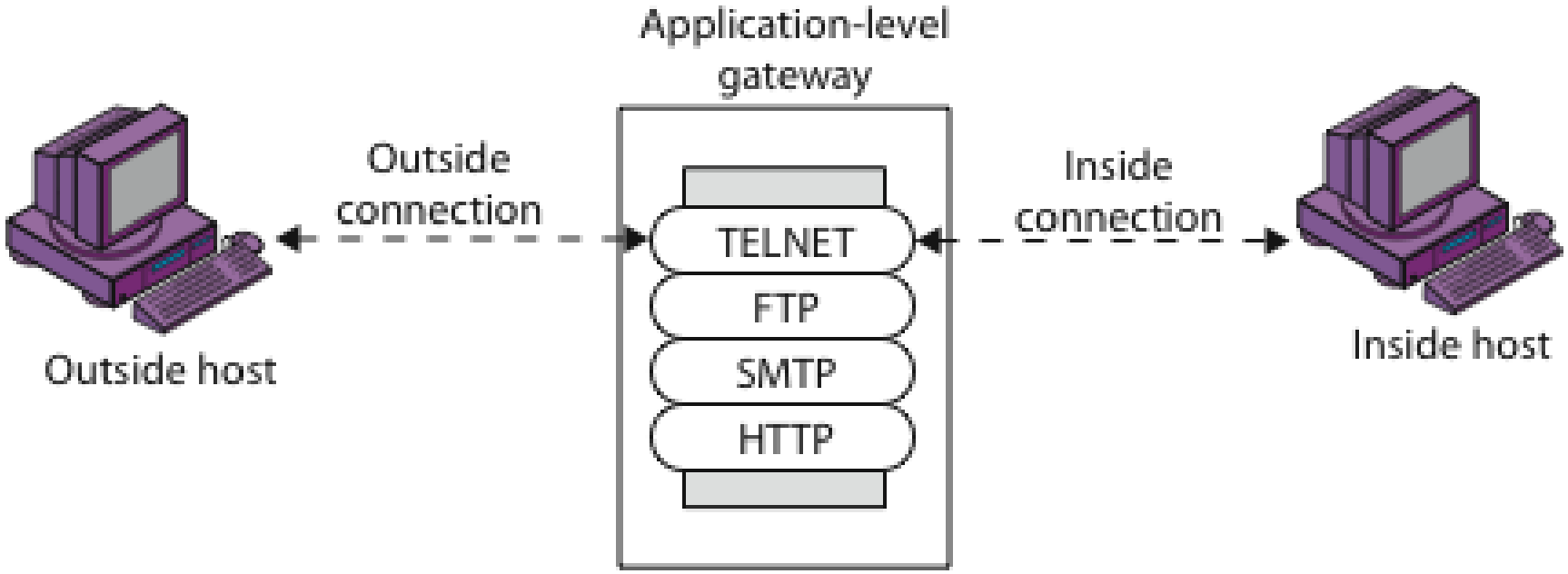
- Người sử dụng yêu cầu dịch vụ từ proxy
- Proxy kiểm tra các yêu cầu có hợp lệ không
- Sau đó xử lý yêu cầu và trả lời cho người sử dụng
- Có thể vào/theo dõi vận chuyển ở tầng ứng dụng

4. Cổng ứng dụng

Cần các proxies khác nhau cho mỗi dịch vụ

- Một số dịch vụ hỗ trợ một cách tự nhiên proxy
- Những loại khác thì cần giải quyết một số vấn đề

4. Cổng ứng dụng

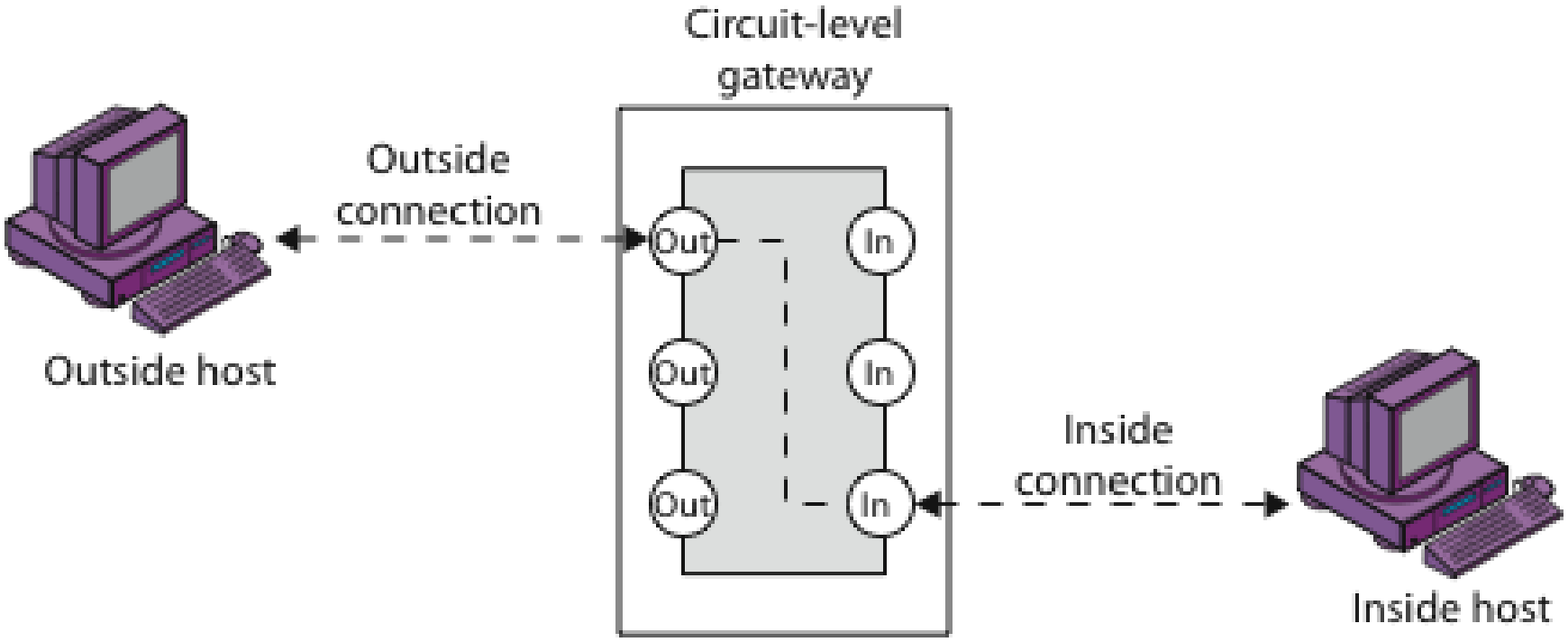


(b) Application-level gateway

5. Cổng giao tiếp mức mạch vòng

- Chuyển tiếp 2 kết nối TCP.
- Có sự an toàn bằng cách hạn chế mà các kết nối này cho phép.
- Mỗi lần tạo ra chuyển tiếp thông thường mà không kiểm tra nội dung.
- Thông thường được sử dụng khi tin cậy người sử dụng bên trong bằng cách cho phép các kết nối ra ngoài nói chung.

5. Cổng giao tiếp mức mạch vòng



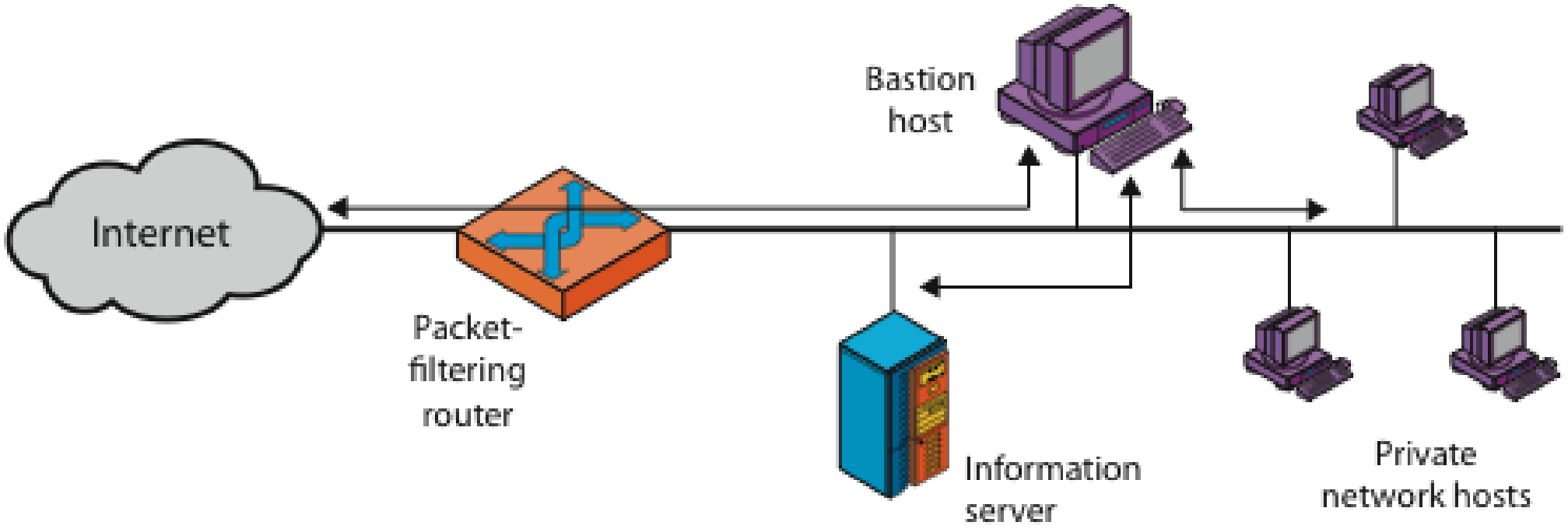
(c) Circuit-level gateway

6. Máy chủ Bastion

- Hệ thống máy chủ an toàn cao.
- Chạy cổng giao tiếp mức ứng dụng và mạch vòng. Hoặc cung cấp các dịch vụ truy cập bên ngoài.
- Có tiềm năng thể hiện các yếu tố của máy chủ.
- Vì an toàn bền vững, nên hệ điều hành nặng nề hơn, các dịch vụ chính, bổ sung xác thực, proxies nhỏ, an toàn, độc lập, không đặc quyền.

6. Máy chủ Bastion

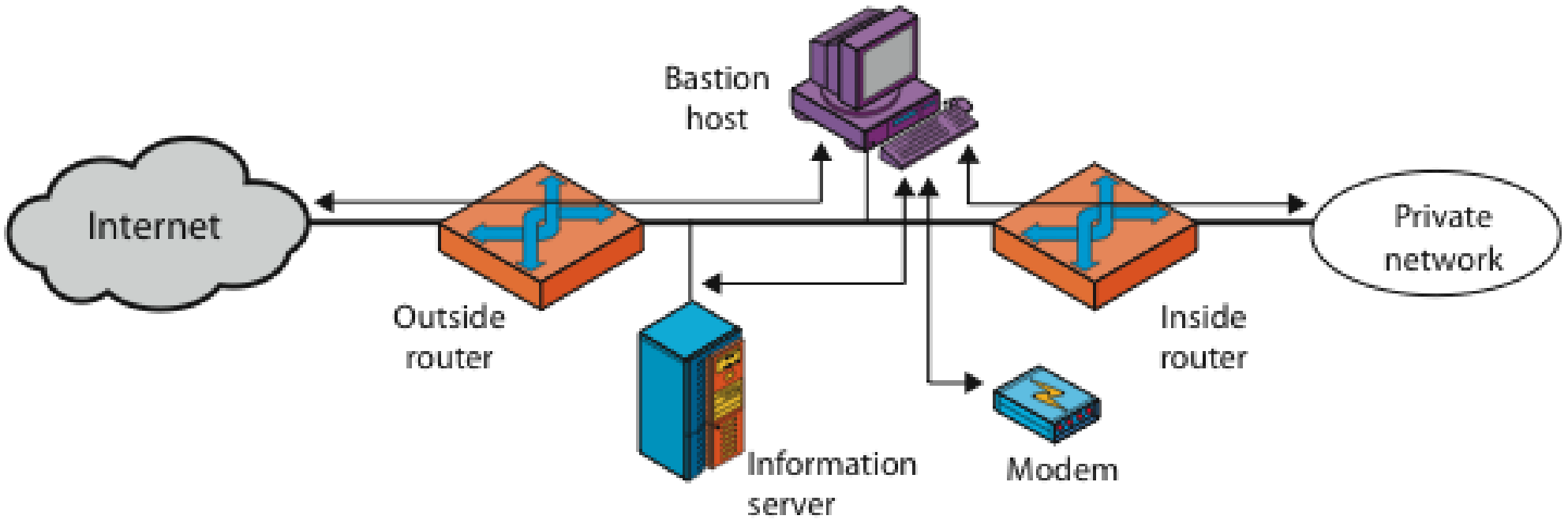
- Cấu hình bức tường lửa



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

6. Máy chủ Bastion

- Cấu hình bức tường lửa



(c) Screened-subnet firewall system

7. Điều khiển truy cập

Điều khiển truy cập (AC: access control) là quyết định xem người dùng có thể làm gì và như thế nào trong hệ thống này.

Một hệ thống cơ bản sẽ bao gồm các thành phần sau:

- Chủ thể - thực thể chủ động (người sử dụng, quá trình)
- Đối tượng - thực thể bị động (file hoặc nguồn)
- Quyền truy cập – cách mà đối tượng được truy cập

7. Điều khiển truy cập

Điều khiển truy cập (AC: access control) là quyết định xem người dùng/ tiến trình có thể làm gì và như thế nào trong hệ thống này.

Một hệ thống cơ bản sẽ bao gồm các thành phần sau:

- Chủ thể - thực thể chủ động (người sử dụng, tiến trình)
- Đối tượng - thực thể bị động (file hoặc nguồn)
- Quyền truy cập – cách mà đối tượng được truy cập

7. Điều khiển truy cập

Ma trận điều khiển quyền truy cập (Access Control Matrix, ACM)

	Program1	. . .	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
. . .				

(a) Access matrix

7. Điều khiển truy cập

- Không thể cài đặt trực tiếp ACM với đầy đủ các thành phần:
  - Số lượng tài nguyên cần phải quản lý quá lớn
  - Kích thước ma trận tăng → tăng bộ nhớ lưu trữ, thời gian tìm kiếm

- Cài đặt gián tiếp ACM:
  - Phân rã theo cột: Danh sách điều khiển truy cập (Access Control List - ACL)
  - Phân rã theo dòng: Danh sách năng lực (Capability List - CL)

8. Các hệ thống máy tính tin cậy

Có các mức độ khác nhau về sự nhạy cảm của thông tin

- Phân loại thông tin quân sự: bảo mật, bí mật

Chủ thể (người hoặc chương trình) có nhiều quyền khác nhau truy cập đến các đối tượng thông tin. Được biết như an toàn nhiều tầng

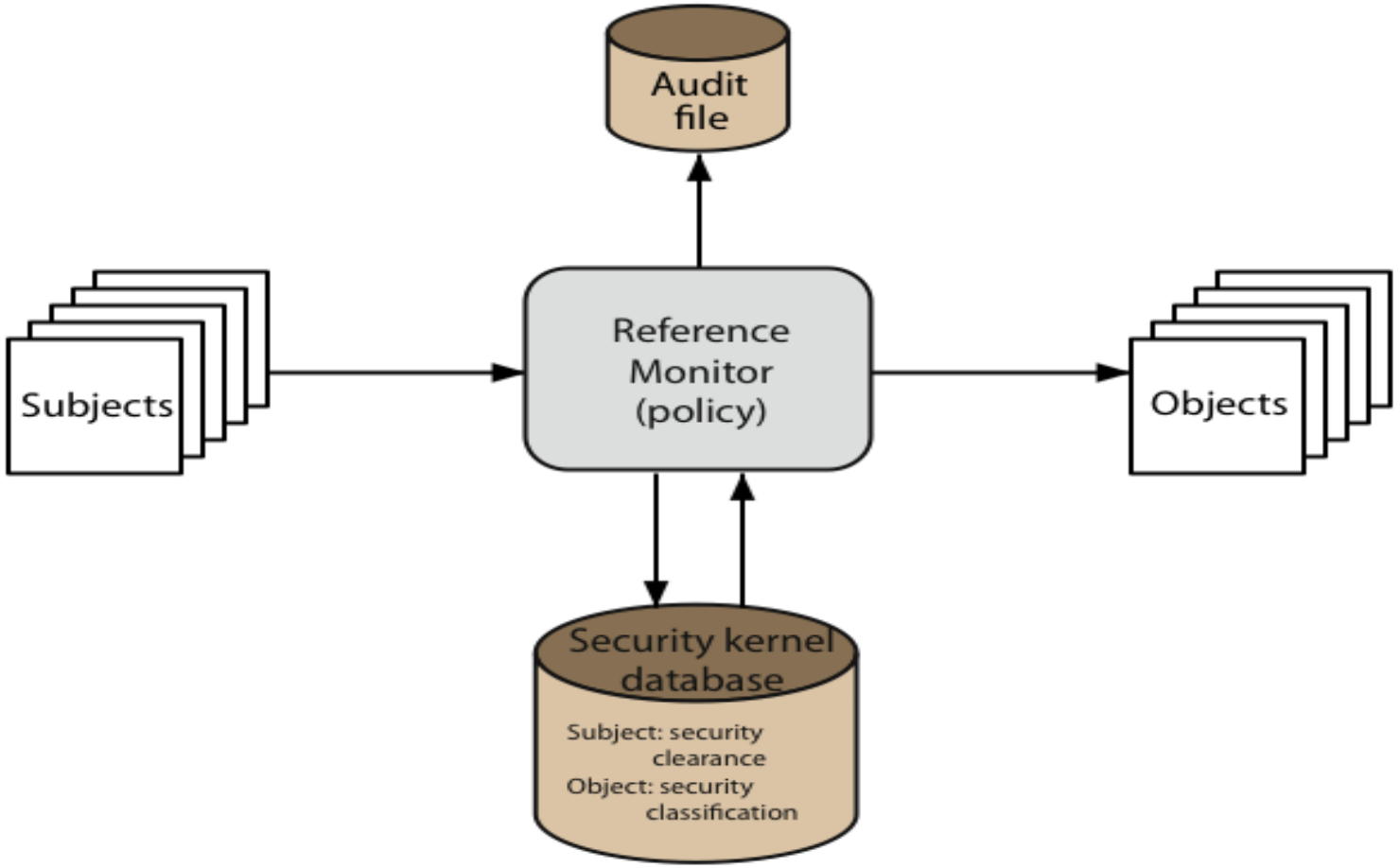
- Chủ thể có mức độ an toàn tối đa và hiện tại
- Đối tượng có phân loại mức độ tin cậy cố định

9. Mô hình Bell LaPadula

- Một trong những mô hình an toàn nổi tiếng nhất. Được cài đặt như các chính sách bắt buộc trong hệ thống.
- Có 2 chính sách chính:
  - Không đọc lên (tính chất an toàn đơn giản)
    - **No read up**: một chủ thể chỉ có thể đọc các dữ liệu có mức độ truy cập **thấp hơn hoặc bằng** với mức độ truy cập của bản thân
  - Không viết xuống (tính chất an toàn ngôi sao)
    - **No write down**: một chủ thể chỉ có thể ghi các dữ liệu có mức độ truy cập **cao hơn hoặc bằng** với mức độ truy cập của bản thân

9. Mô hình Bell LaPadula

Có thể coi Firewall như một bộ máy giám sát (Reference monitor)



10. Tiêu chuẩn chung

- Đặc tả yêu cầu an toàn quốc tế khởi đầu và xác định tiêu chuẩn triển khai. Tích hợp với các chuẩn khác
  - Chẳng hạn CSEC, ITSEC, CTCPEC (Canada), Federal (US)

- Đặc tả các chuẩn cho
  - Tiêu chuẩn triển khai
  - Phương pháp luận cho ứng dụng của Tiêu chuẩn
  - Các thủ tục hành chính triển khai, chứng nhận và các sơ đồ chỉ định

10. Tiêu chuẩn chung

- Xác định tập các yêu cầu an toàn, có đích triển khai (TOE). Yêu cầu rơi vào trong 2 loại sau
  - Chức năng
  - Sự tin cậy

  Cả hai được tổ chức theo lớp classes của họ hoặc cấu thành

10. Tiêu chuẩn chung

Các yêu cầu Tiêu chuẩn chung

- Yêu cầu chức năng
  - Kiểm soát an toàn, hỗ trợ mã, trao đổi thông tin, bảo vệ dữ liệu người sử dụng, định danh và xác thực, quản lý an toàn, tính riêng tư, bảo vệ các hàm an toàn tin cậy, nguồn thiết thực, truy cập TOE, đường dẫn tin cậy
- Yêu cầu sự tin cậy
  - Quản lý tham số hệ thống, phân phối và thao tác, phát triển, tài liệu chỉ dẫn, hỗ trợ thời gian sống, kiểm tra, đánh giá lỗ hổng, bảo trì sự tin cậy

7.3 Mạng riêng ảo VPN

1. Mạng riêng ảo VPN là gì?

- Mạng riêng ảo (Virtual Private Network, VPN) là một chuẩn công nghệ cung cấp sự liên lạc riêng tư giữa 2 thực thể trên mạng công khai (ví dụ như Internet).
- VPN giả lập một mạng riêng trên mạng công cộng dựa trên các liên kết ảo.
- VPN được sử dụng để truyền dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng.
- VPN hoạt động bằng cách ẩn địa chỉ IP của người dùng và mã hóa dữ liệu để chỉ người được cấp quyền nhận dữ liệu mới có thể đọc được.

2. Công dụng của VPN

1. Quyền riêng tư: Người ngoài cuộc khó có thể hiểu được nội dung liên lạc. VPN sử dụng mã hóa để giữ bí mật dữ liệu cá nhân như mật khẩu, thông tin thẻ tín dụng và lịch sử duyệt web.

2. Tính ẩn danh: Kết nối VPN sẽ ẩn địa chỉ IP của bạn, để bạn được ẩn danh trên Internet.

3. Bảo mật: Dịch vụ VPN sử dụng mật mã để bảo vệ kết nối Internet của bạn khỏi những truy cập trái phép. VPN cũng có thể hoạt động như một cơ chế tắt, hủy bỏ các chương trình được chọn trước đó phòng khi có hoạt động đáng ngờ trên Internet. Những tính năng trên cho phép các công ty cấp quyền truy cập từ xa cho người dùng được ủy quyền thuộc mạng lưới kinh doanh của họ.

3. Hoạt động của VPN

Kết nối VPN chuyển hướng các gói dữ liệu từ máy của bạn tới một máy chủ từ xa khác trước khi gửi chúng cho các bên thứ ba qua Internet. Các nguyên tắc chính đằng sau công nghệ VPN bao gồm:

a) Giao thức đường hầm

b) Mã hóa

c) Thỏa thuận về chất lượng dịch vụ

a) Giao thức đường hầm

- Đường hầm là cơ chế dùng để đóng gói một giao thức vào trong một giao thức khác.
- VPN tạo ra đường hầm dữ liệu bảo mật giữa máy cục bộ của bạn và một máy chủ VPN khác ở cách xa bạn hàng ngàn cây số.
- Khi bạn truy cập mạng, máy chủ VPN này trở thành nguồn chung cho tất cả dữ liệu của bạn. Nhà cung cấp dịch vụ Internet (ISP) của bạn và các bên thứ ba khác sẽ không thể xem nội dung lưu lượng Internet của bạn nữa.

b) Mã hóa

- Giao thức VPN như IPSec làm nhiễu dữ liệu của bạn trước khi gửi chúng qua đường hầm dữ liệu.
- Dịch vụ VPN hoạt động như một bộ lọc, khiến dữ liệu của bạn trở nên không thể đọc được ở một đầu và chỉ giải mã dữ liệu ở đầu bên kia. Việc này ngăn ngừa hành vi sử dụng dữ liệu cá nhân trái phép, kể cả khi kết nối mạng của bạn bị xâm phạm.
- Lưu lượng mạng trở nên khó bị tấn công và kết nối Internet của bạn được bảo mật

c) Thỏa thuận về chất lượng dịch vụ

- Thỏa thuận về chất lượng dịch vụ (QoS: Quality of Service) định ra giới hạn cho phép về độ trễ trung bình của gói tin trong mạng.

4. Tại sao bạn nên sử dụng VPN?

- Truy cập Internet công cộng an toàn. VPN giúp hoạt động truy cập web ở mọi lúc, mọi nơi trở nên an toàn hơn cho tất cả mọi người.
- Đảm bảo sự riêng tư cho lịch sử tìm kiếm của bạn. ISP và trình duyệt web theo dõi lịch sử tìm kiếm của bạn. Kết nối VPN sẽ bảo vệ dữ liệu của bạn không bị sử dụng trái phép.

4. Tại sao bạn nên sử dụng VPN?

- Truy cập dịch vụ phát trực truyến trên toàn cầu. Khi bạn rời khỏi quốc gia của mình, dịch vụ phát trực tuyến có trả phí của bạn có thể không hoạt động do điều khoản và quy định trong hợp đồng. Kết nối VPN cho phép bạn thay đổi địa chỉ IP từ quốc gia của bạn và truy cập vào những chương trình ưa thích từ nơi bạn đang ở.
- Bảo vệ danh tính của bạn. Bằng cách ẩn đi danh tính của bạn, dịch vụ VPN bảo vệ bạn trước sự giám sát kỹ thuật số.

5. Làm thế nào để thiết lập VPN?

Có 2 cách phổ biến để truy cập vào dịch vụ VPN cho cá nhân:

1. Sử dụng nhà cung cấp dịch vụ VPN

2. Sử dụng bộ định tuyến VPN

5. Làm thế nào để thiết lập VPN?

1. Sử dụng nhà cung cấp dịch vụ VPN
   - Có thể lựa chọn một dịch vụ VPN có thể được truy cập thông qua trình duyệt hoặc bằng cách tải ứng dụng hay phần mềm về thiết bị của bạn.
   - Có các dịch vụ theo gói đăng ký thường sẽ tính phí dựa trên mỗi thiết bị sử dụng dịch vụ.
   - Do vậy, việc thiết lập các dịch vụ này có thể khá tốn kém. Đồng thời, mỗi thiết bị lại cần được cấu hình riêng biệt.

5. Làm thế nào để thiết lập VPN?

2. Sử dụng bộ định tuyến VPN

- Bao gồm mua bộ định tuyến được cài đặt trước kết nối VPN hoặc tự cài phần mềm VPN trên bộ định tuyến tại nhà của bạn.
- Ưu điểm của cách tiếp cận này là tất cả các thiết bị truy cập vào Internet thông qua bộ định tuyến này sẽ được bảo vệ tự động.

6. Chọn được nhà cung cấp VPN tốt nhất?

Hãy sử dụng danh sách bên dưới để đánh giá các nhà cung cấp dịch vụ VPN

1. Chính sách ghi nhật ký: Những nhà cung cấp VPN tốt nhất có chính sách ghi nhật ký tối thiểu hoặc không ghi để ngăn ngừa rò rỉ thông tin từ phía họ.

2. Phần mềm được cập nhật: Kết nối VPN tốt nhất sẽ sử dụng giao thức đường hầm mới nhất. Giao thức OpenVPN đem lại khả năng bảo mật mạnh mẽ hơn so với các giao thức khác. Giao thức này là phần mềm có mã nguồn mở, tương thích với tất cả hệ điều hành phổ biến.

6. Chọn được nhà cung cấp VPN tốt nhất?

Hãy sử dụng danh sách bên dưới để đánh giá các nhà cung cấp dịch vụ VPN

3. Giới hạn băng thông: Tất cả các dịch vụ đều có hạn mức sử dụng dữ liệu. Bạn sẽ cần chọn một nhà cung cấp dịch vụ VPN đáp ứng nhu cầu dữ liệu của bạn trong tầm ngân sách.

4. Vị trí máy chủ VPN: Bạn phải đảm bảo rằng nhà cung cấp dịch vụ VPN của bạn có máy chủ đặt ở quốc gia mà bạn yêu cầu quyền truy cập Internet riêng tư.

7. Lựa chọn giữa VPN có trả phí và miễn phí?

- VPN miễn phí sẽ hữu ích nếu bạn có ngân sách hạn chế.
- Tuy nhiên, bạn cần lưu ý rằng nguồn doanh thu chính của nhà cung cấp dịch vụ VPN miễn phí đến từ quảng cáo.
- Bạn nên dự tính việc bị quảng cáo nhắm mục tiêu hoặc chính sách ghi nhật ký và bán dữ liệu được giấu trong điều khoản và điều kiện sử dụng.

7. Lựa chọn giữa VPN có trả phí và miễn phí?

- Hầu hết các dịch vụ VPN miễn phí:

✓ Không cung cấp giao thức VPN mới nhất

✓ Không có hỗ trợ kỹ thuật chất lượng tốt

✓ Có băng thông thấp và tốc độ chậm hơn cho người dùng miễn phí

✓ Có phí ngắt kết nối cao hơn

✓ Phân bổ số lượng máy chủ VPN bị giới hạn về mặt địa lý

8. Tại sao doanh nghiệp sử dụng VPN?

- VPN là cách thức tiết kiệm chi phí, tốc độ cao và bảo mật để kết nối người dùng từ xa với mạng văn phòng.
- Vì kết nối VPN thường được thực hiện trên mạng Internet công cộng, chúng có thể rẻ tiền hơn và có mức băng thông cao hơn so với liên kết WAN (mạng diện rộng) chuyên dụng hoặc liên kết đường dài, quay số từ xa.
- So với liên kết LAN hoặc WAN chuyên dụng và đắt đỏ hay liên kết đường dài, quay số từ xa, kết nối VPN cung cấp khả năng truy cập Internet riêng tư với băng thông cao cho các công ty.

9. Doanh nghiệp sử dụng VPN như thế nào?

Các doanh nghiệp sử dụng VPN theo 3 cách thức chính như sau:

a) Site to site VPN

b) Client VPN hay Open VPN

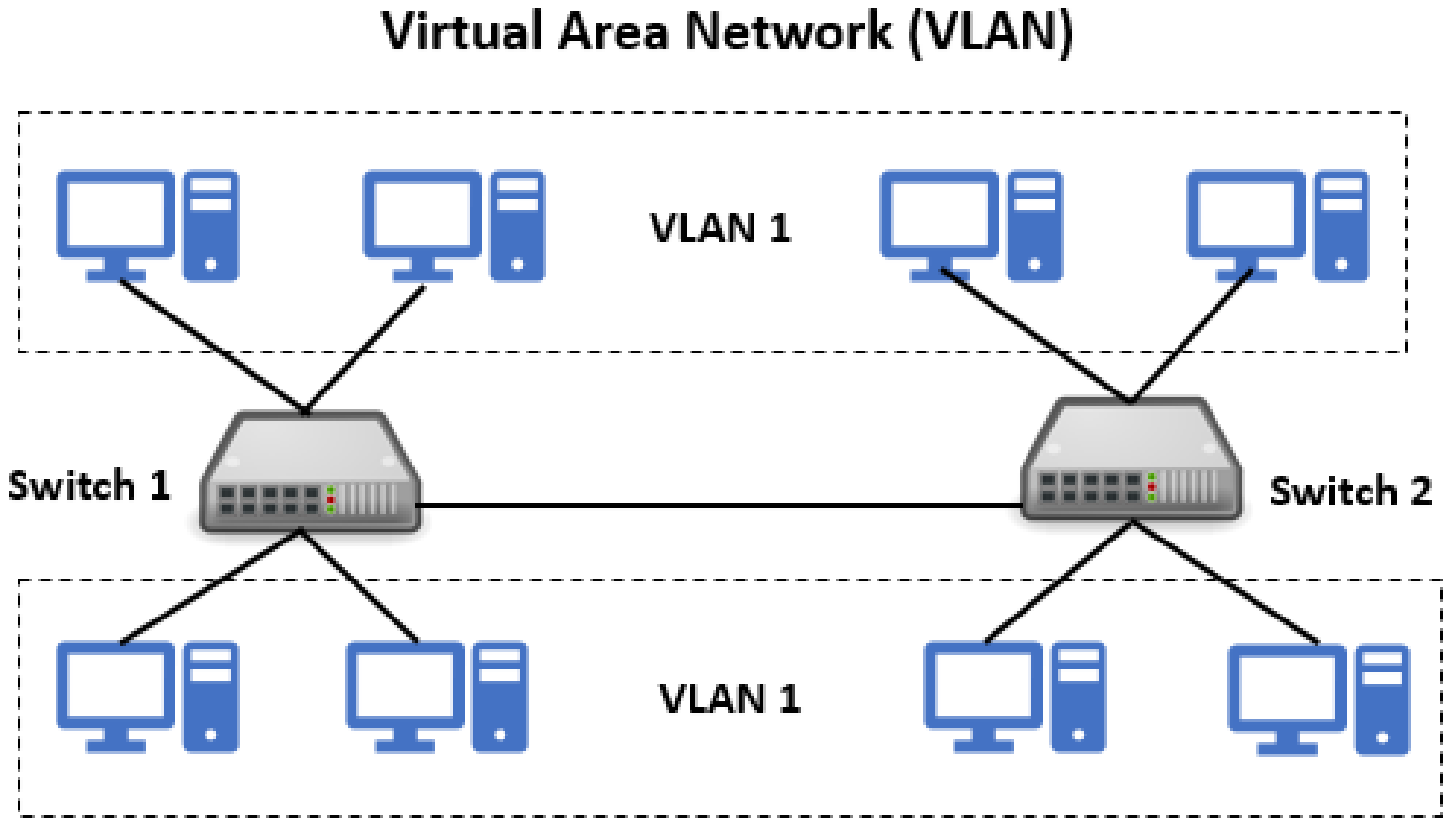
c) SSL VPN

10. Làm thế nào để sử dụng AWS VPN?

- AWS VPN cung cấp hai dịch vụ quý giá: VPN site-to-site của AWS và VPN máy khách của AWS.
- AWS Site-to-Site VPN cho phép bạn kết nối mạng lưới tại chỗ hoặc tại địa điểm văn phòng chi nhánh một cách an toàn tới Amazon Virtual Private Cloud (Amazon VPC) của bạn.
- AWS Client VPN giúp bạn kết nối người dùng một cách an toàn tới AWS hoặc mạng lưới tại chỗ

7.4 VLAN

VLAN (Virtual Local Area Network - mạng LAN ảo), là một mạng tuỳ chỉnh, được hình thành từ một hoặc nhiều mạng LAN, cho phép các nhóm thiết bị khả dụng kết nối cùng với một mạng dù không đặt cạnh nhau.



1. VLAN 1 là gì?

- Là kiểu mạng mặc định của tất cả các thiết bị chuyển mạch hỗ trợ VLAN và nó hoạt động ở Lớp 2 (Data Link layer) trong mô hình OSI của hệ thống,
- Nếu hệ thống mạng máy tính của bạn được trang bị một thiết bị chuyển mạch có hỗ trợ chức năng này mà bạn chưa thiết lập các thông số kỹ thuật thì mặc định nó vẫn có thể chuyển tiếp các gói dữ liệu giữa các máy tính và thiết bị kết nối vào nó một cách bình thường như các thiết bị chuyển mạch khác
- Lúc này tất cả các cổng mạng trên thiết bị chuyển mạch mặc định đều nằm trong cùng một miền quảng bá và với sự quản lý của VLAN 1.

2. Default VLAN là gì?

- Là kiểu VLAN mặc định ban đầu với tất cả các cổng giao tiếp trên thiết bị chuyển mạch
- Default VLAN cũng có thể hiểu là VLAN 1, và các VLAN khác như User VLAN, Native VLAN, Management VLAN đều là các thành phần con của Default VLAN

3. User VLAN (hay Data VLAN) là gì?

Là VLAN trong đó chứa các tài khoản người dùng thành từng nhóm dựa theo các thuộc tính về đặc thù công việc của từng nhóm làm việc hay theo thuộc tính về vị trí vật lý của các nhóm làm việc này.

4. Native VLAN là gì?

- Là VLAN dùng để cấu hình Trunking do một số thiết bị không tương thích với nhau, lúc này ta phải sử dụng Native VLAN để chúng có thể giao tiếp với nhau.
- Khi đó, tất cả các khung dữ liệu (frame) của các VLAN khi giao tiếp qua kết nối Trunking đều sẽ được gắn tag của giao thức 802.1Q hoặc ISL, ngoại trừ các frame của VLAN 1.
- Native VLAN là VLAN mà frame của nó sẽ không được tag trước khi gửi qua đường trunk. Ngầm định Native VLAN của Switch là VLAN 1.

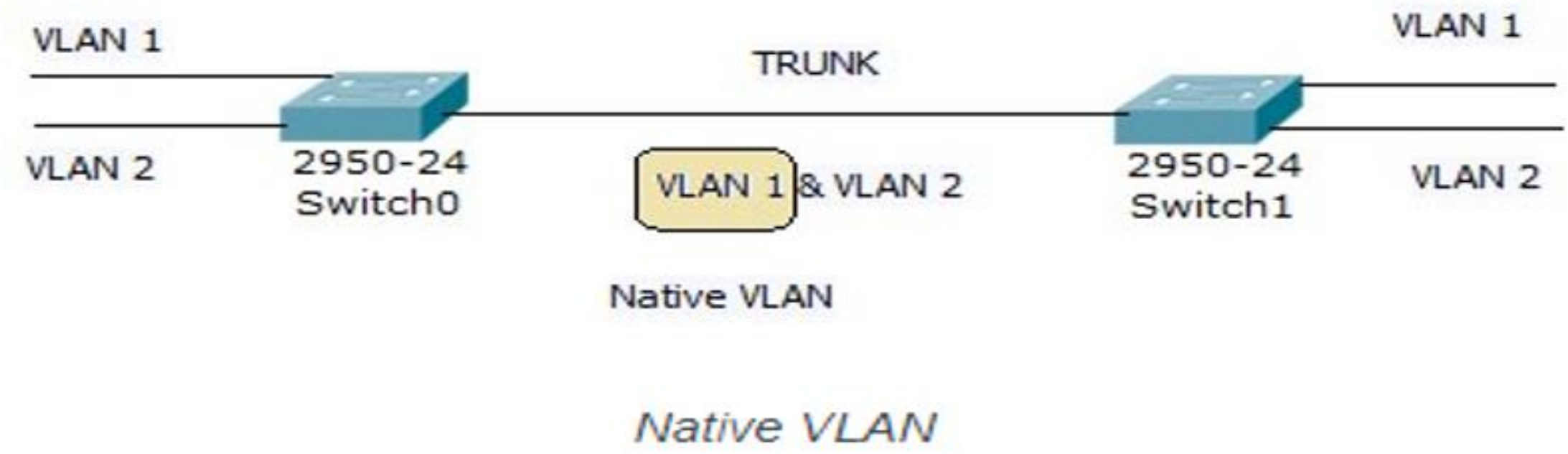
4. Native VLAN là gì?

❖ Cấu hình Native VLAN như sau:

- *Switch#config terminal*
- *Switch(config)#interface fastethernet slot/port_number*
- *Switch(config-if)#switchport trunk native vlan* ***vlan-id***

❖ Trong đó **vlan-id** là chỉ số của VLAN native.

4. Native VLAN là gì?



5. Management VLAN là gì?

- Để có thể giám sát từ xa các thiết bị chuyển mạch trong hệ thống mạng của mình, bạn cần phải có một VLAN đặc biệt dùng để thực hiện việc này, đó chính là Management VLAN.
- Bằng cách gán một địa chỉ IP dùng để telnet từ xa vào hệ thống mạng thông qua địa chỉ IP này, và có thể cấm các người dùng khác truy cập vào thiết bị. Vì đây là một VLAN khá nhạy cảm được cấp một số quyền quản trị nên nó cần phải được tách riêng ra khỏi các VLAN khác để đảm bảo yếu tố an toàn bảo mật. Khi mạng có vấn đề như: hội tụ với STP, broadcast storms thì một Management VLAN cho phép nhà quản trị vẫn có thể truy cập được vào thiết bị và giải quyết vấn đề đó.

5. Management VLAN là gì?

❖ Cấu hình địa chỉ IP cho Switch như sau:

- *Switch#config terminal*
- *Switch(config)#interface vlan vlan-id*
- *Switch(config-if)#ip address xxx.xxx.xxx.xxx subnet mask*
- *Switch(config-if)#end*

❖ Địa chỉ này sẽ được sử dụng để quản trị Switch từ xa (qua telnet). xxx.xxx.xxx.xxx là địa chỉ IP của VLAN. Ví dụ: 192.168.10.2 Ví dụ subnet mask là 255.255.255.0

6. Voice VLAN là gì?

- Là VLAN dành cho lưu lượng thoại.
- Nó cho phép các cổng Switch mang lưu lượng thoại IP từ một điện thoại IP.
- Người quản trị mạng cấu hình một Voice VLAN và gán nó để truy cập các cổng.
- Khi một điện thoại IP được kết nối với các cổng Switch, Switch sẽ gửi gói tin CDP đó hướng dẫn các điện thoại IP đính kèm để gửi lưu lượng thoại được gán nhãn VLAN ID.

6. Voice VLAN là gì?

7.5 NAT

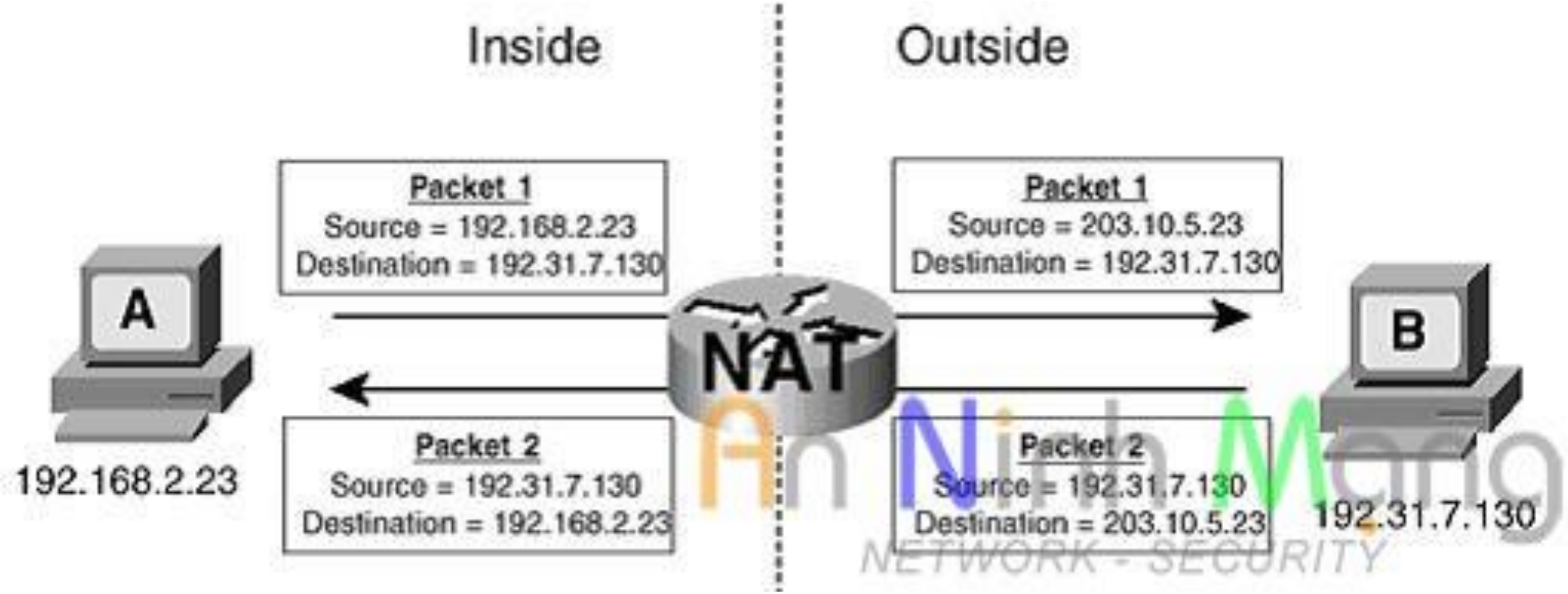
1. Khái niệm NAT

- NAT (Network Address Translation) là một kỹ thuật chuyển đổi IP nội miền sang IP ngoại miền.
- Mạng lưới internet toàn cầu ngày một phát triển mạnh mẽ. Có khoảng trên 100 triệu host, toàn cầu tính đến đầu năm 2021 sớm đặt mốc 4.66 tỷ người.
- Tốc độ phát triển nóng như vậy lại càng đòi hỏi sự tham gia của kỹ thuật NAT. Nhờ có kỹ thuật này, mạng cục bộ LAN sẽ mở rộng liên kết nối tiếp thuận lợi hơn.

7.5 NAT

1. Khái niệm NAT

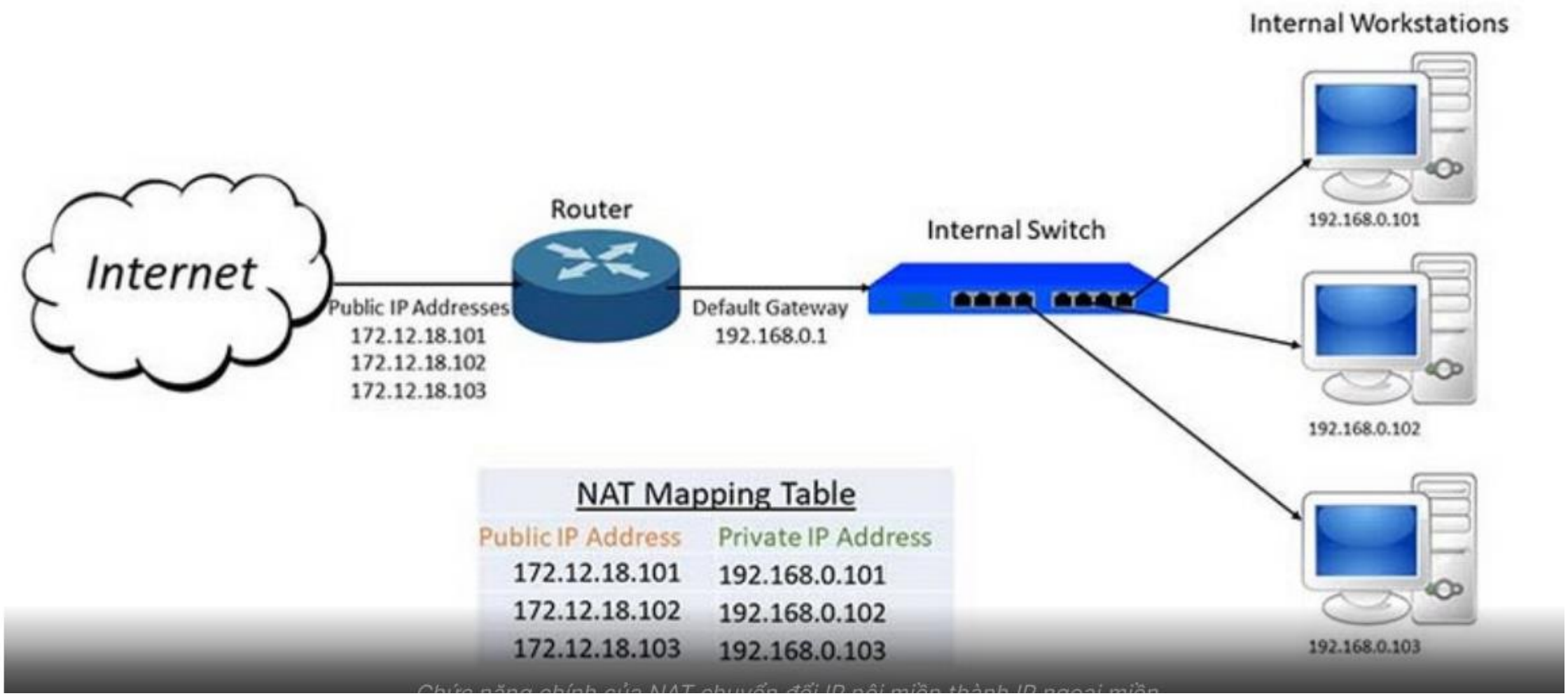
Ví dụ NAT



2. Chức năng chính của NAT

- Trong một hệ thống mạng NAT giữ vai trò di chuyển gói tin giữa các lớp mạng khác nhau. Cụ thể, NAT cần tiến hành chuyển đổi địa chỉ IP trong từng gói tin và chuyển đến router cùng một số thiết bị mạng khác.
- Trong quá trình chuyển gói tin từ mạng công cộng public ngược lại NAT, NAT cần tiến hành thay đổi IP đích sang dạng IP nội bộ. Sau đó mới chuyển đi.
- Mặt khác, NAT còn hoạt động tương tự như một từờng lửa, hỗ trợ bảo mật IP của thiết bị. Giả sử máy tính bị gián đoạn khi kết nối với internet, IP public khi đó lập tức chuyển đổi thành IP thay thế mạng cục bộ.

2. Chức năng chính của NAT



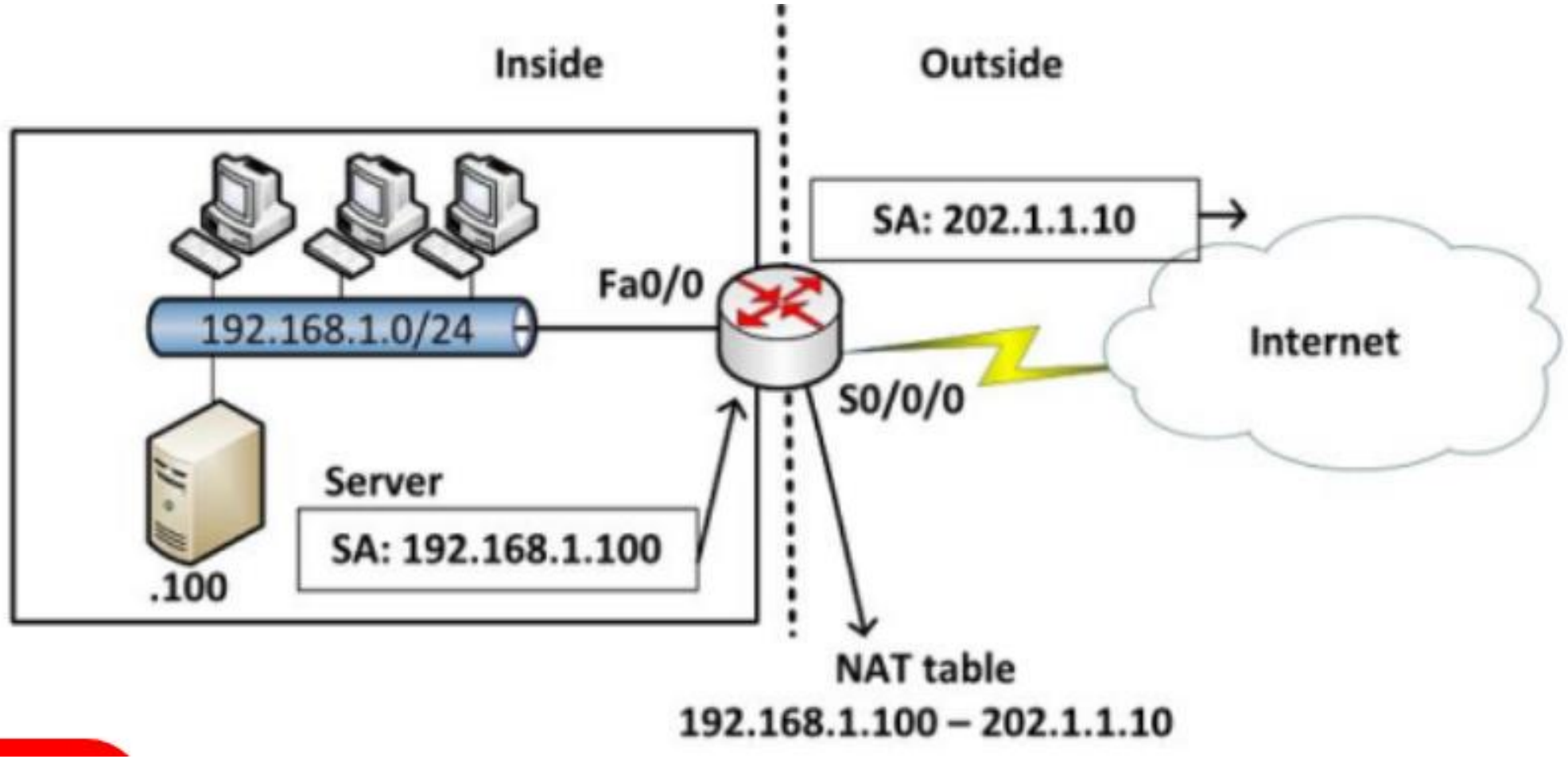
Chức năng chính của NAT chuyển đổi IP nội miền thành IP ngoại miền

3. Static NAT

- Static NAT được dùng để chuyển đổi một địa chỉ IP này sang một địa chỉ khác một cách cố định, thông thường là từ một địa chỉ cục bộ sang một địa chỉ công cộng và quá trình này được cài đặt thủ công, nghĩa là địa chỉ ánh xạ và địa chỉ ánh xạ chỉ định rõ ràng tương ứng duy nhất.
- Static NAT rất hữu ích trong trường hợp những thiết bị cần phải có địa chỉ cố định để có thể truy cập từ bên ngoài Internet. Những thiết bị này phổ biến là những Server như Web, Mail,...
- Ví dụ:
  - Router (config) # ip nat inside source static 192.168.1.100 202.1.1.10
  - Router (config) # interface fa0/0
  - Router (config-if) # ip nat inside
  - Router (config) # interface s0/0/0
  - Router (config-if) # ip nat outside

3. Static NAT

Ví dụ cấu hình Static NAT

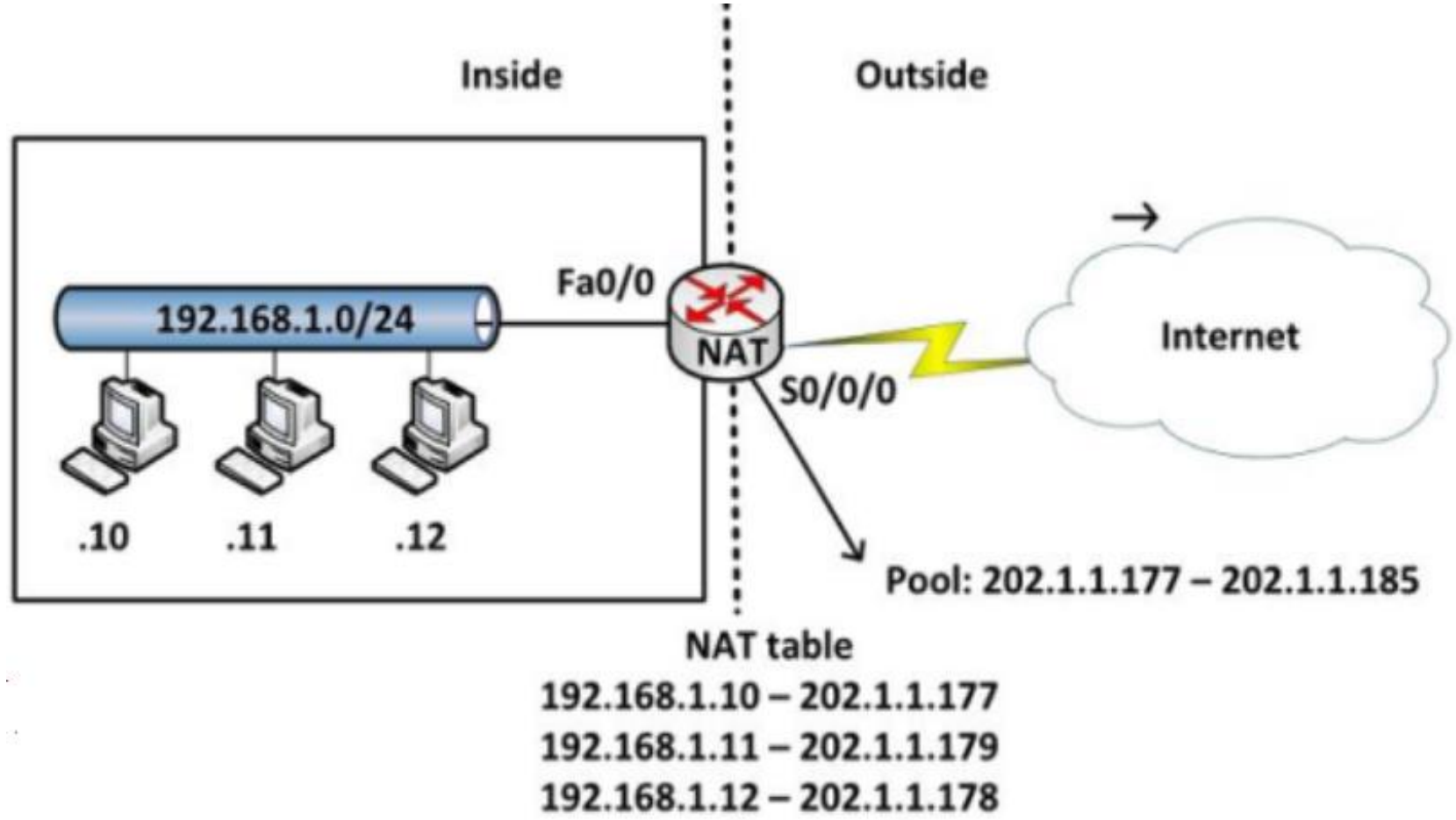


4. Dynamic NAT

- Dynamic NAT được dùng để ánh xạ một địa chỉ IP này sang một địa chỉ khác một cách tự động, thông thường là ánh xạ từ một địa chỉ cục bộ sang một địa chỉ được đăng ký. Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán một thiết bị bên trong mạng.
- Ví dụ:
  - Router (config) # ip nat pool abc 202.1.1.177 202.1.1.185 netmask 255.255.255.0
  - Router (config) # access-list 1 permit 192.168.1.0 0.0.0.255
  - Router (config) # ip nat inside source list 1 pool abc
  - Router (config) # interface fa0/0
  - Router (config-if) # ip nat inside
  - Router (config) # interface s0/0/0
  - Router (config-if) # ip nat outside

4. Dynamic NAT

Ví dụ Dynamic NAT

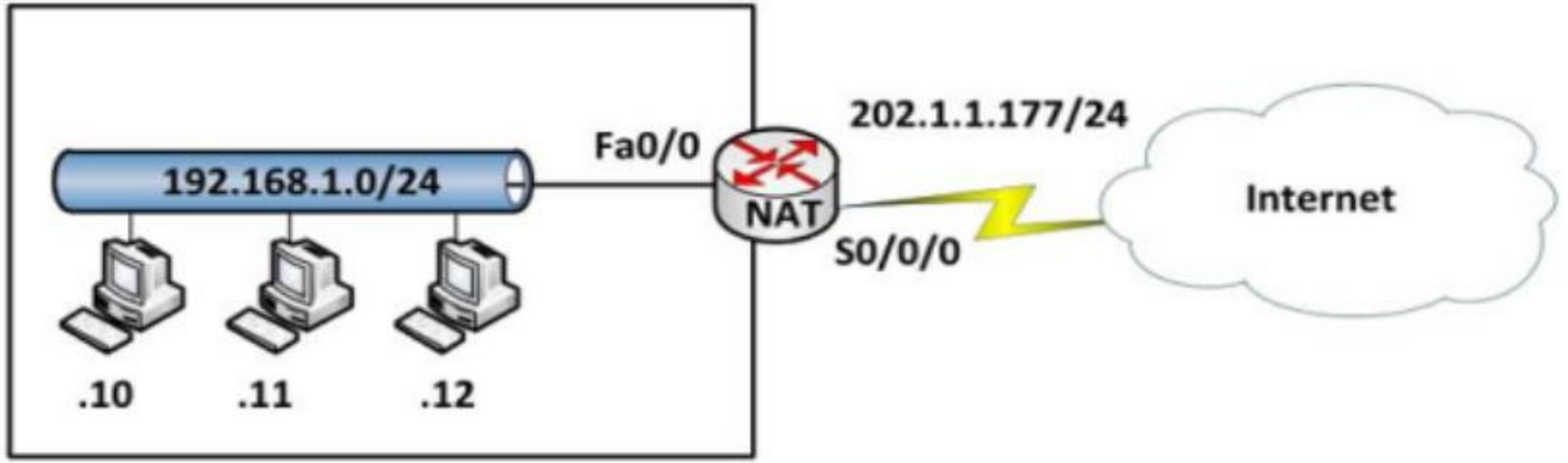


5. NAT overload

- NAT Overload là một dạng của Dynamic NAT, nó thực hiện ánh xạ nhiều địa chỉ IP thành một địa chỉ (many - to - one) và sử dụng các địa chỉ số cổng khác nhau để phân biệt cho từng chuyển đổi. NAT Overload còn có tên gọi là PAT (Port Address Translation).
- Chỉ số cổng được mã hóa 16 bit, do đó có tới 65536 địa chỉ nội bộ có thể được chuyển đổi sang một địa chỉ công cộng.
- Ví dụ:
  - Router (config) # access-list 1 permit 192.168.1.0 0.0.0.255
  - Router (config) # ip nat inside source list 1 interface s0/0/0 overload
  - Router (config) # interface fa0/0
  - Router (config-if) # ip nat inside
  - Router (config) # interface s0/0/0
  - Router (config-if) # ip nat outside

5. NAT overload

Ví dụ NAT overload



NAT table

192.168.1.10 – 202.1.1.177:**1030**
192.168.1.11 – 202.1.1.177:**1031**
192.168.1.12 – 202.1.1.177:**1032**