CHƯƠNG 4
CÁC KỸ THUẬT VÀ CÔNG NGHỆ ĐẢM BẢO ATTT

TỔNG QUAN NỘI DUNG

1. Điều khiển truy cập
2. Tường lửa
3. VPN
4. IDS và IPS
5. Honeypot, Honeynet và các hệ thống Padded Cell

1. Điều khiển truy cập

Điều khiển truy cập

1. Khái niệm về điều khiển truy cập
2. Các mô hình điều khiển truy cập
3. Các công nghệ xác thực và nhận dạng người dùng

1.1. Khái niệm về điều khiển truy cập

- Cấp phép hoặc từ chối phê duyệt sử dụng các tài nguyên đã biết
- Cơ chế của hệ thống thông tin cho phép hoặc hạn chế truy cập đến dữ liệu hoặc các thiết bị
- Bốn mô hình tiêu chuẩn
- Các phương pháp thực tiễn để thực thi điều khiển truy cập

1.1. Khái niệm về điều khiển truy cập

- Điều khiển truy cập là quy trình bảo vệ một nguồn lực để đảm bảo nguồn lực này chỉ được sử dụng bởi các đối tượng đã được cấp phép
- Điều khiển truy cập nhằm ngăn cản việc sử dụng trái phép

Các thuật ngữ

- Cấp phép (authorization) nhằm đảm bảo kiểm soát truy nhập tới hệ thống, ứng dụng và dữ liệu
- Nhận diện: Xem xét các ủy quyền
  - Ví dụ: người vận chuyển hàng xuất trình thẻ nhân viên
- Ủy quyền: cấp quyền cho phép
- Xác thực (chứng thực): Kiểm tra, xác minh các ủy quyền
  - Ví dụ: kiểm tra thẻ của người vận chuyển hàng

Các thuật ngữ (tiếp)

- Đối tượng: Tài nguyên cụ thể
  - Ví dụ: file hoặc thiết bị phần cứng
- Chủ thể: Người dùng hoặc quá trình hoạt động đại diện cho một người dùng
  - Ví dụ: người dùng máy tính
- Thao tác: Hành động do chủ thể gây ra đối với một đối tượng
  - Ví dụ: xóa một file

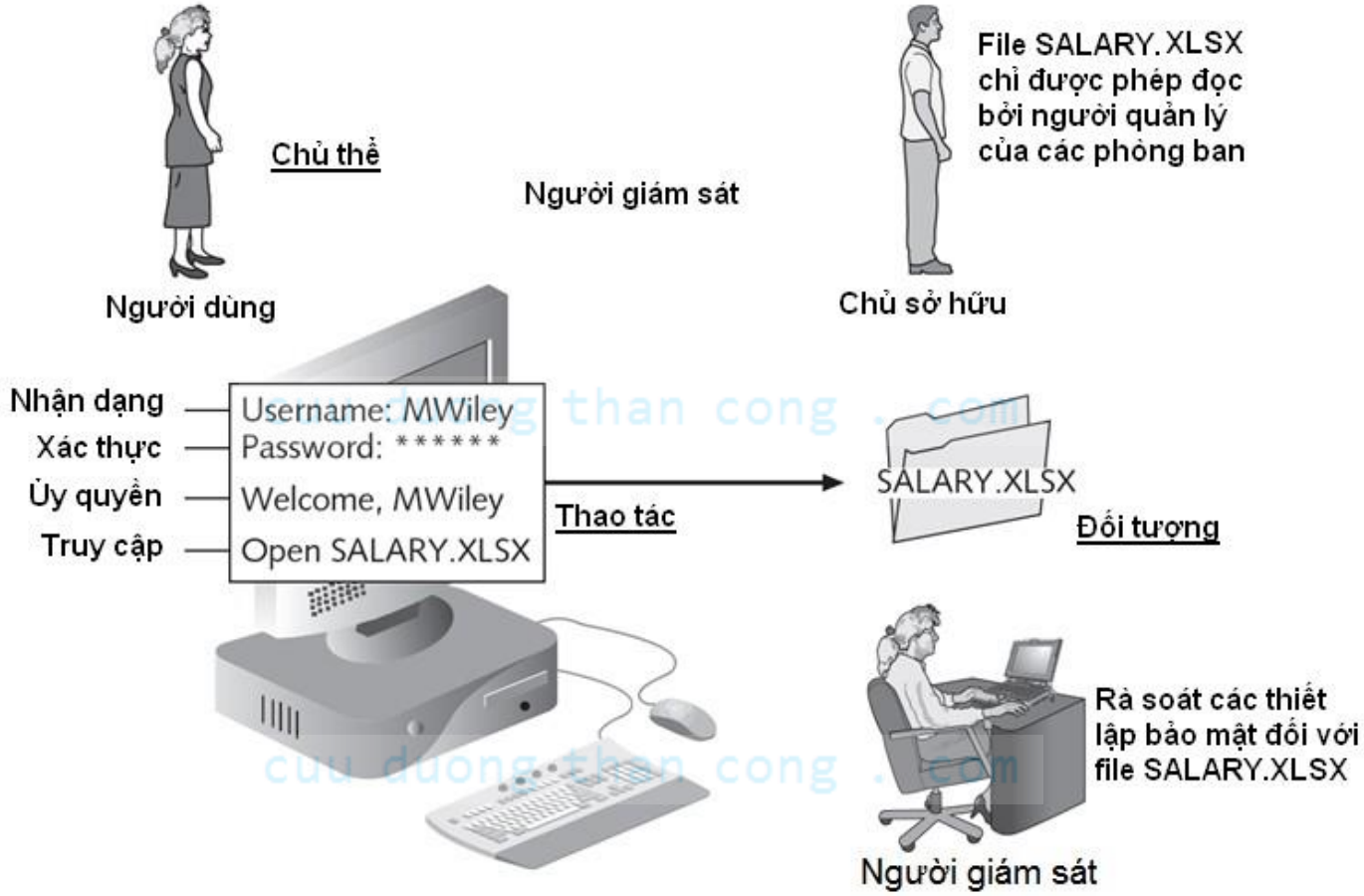
Các bước điều khiển truy cập cơ bản

Hành động	Mô tả	Ví dụ tình huống	Quá trình trên máy tính
Nhận diện	Xem xét các ủy quyền	Người vận chuyển hàng xuất trình thẻ nhân viên	Người dùng nhập tên đăng nhập
Xác thực	Xác minh các ủy quyền có thực sự chính xác hay không	Đọc thông tin trên thẻ để xác định những thông tin đó có thực hay không	Người dùng cung cấp mật khẩu
Ủy quyền	Cấp quyền cho phép	mở cửa cho phép người vận chuyển hàng đi vào	Người dùng đăng nhập hợp lệ
Truy cập	Quyền được phép truy cập tới các tài nguyên xác định	Người vận chuyển hàng chỉ có thể lấy các hộp ở cạnh cửa	Người dùng được phép truy cập tới các dữ liệu cụ thể

Các vai trò trong điều khiển truy cập

Vai trò	Mô tả	Trách nhiệm	Ví dụ
Chủ sở hữu	Người chịu trách nhiệm về thông tin	Xác định mức bảo mật cần thiết đối với dữ liệu và gán các nhiệm vụ bảo mật khi cần	Xác định rằng chỉ những người quản lý của cơ quan mới có thể đọc được file SALARY.XLSX
Người giám sát	Cá nhân mà mọi hành động thường ngày của anh ta do chủ sở hữu quy định	Thường xuyên rà soát các thiết lập bảo mật và duy trì các bản ghi truy cập của người dùng	Thiết lập và rà soát các thiết lập bảomật cho file SALARY.XLSX
Người dùng	Người truy cập thông tin trong phạm vi trách nhiệm được giao phó	Tuân thủ đúng các chỉ dẫn bảo mật của tổ chức và không được cố ý vi phạm bảo mật	Mở file SALARY.XSLX

Các vai trò trong điều khiển truy cập (tiếp)



1.2. Các mô hình điều khiển truy cập

- Các tiêu chuẩn cung cấp nền tảng cơ sở (framework) được định trước cho các nhà phát triển phần cứng hoặc phần mềm
- Được sử dụng để thực thi điều khiển truy cập trong thiết bị hoặc ứng dụng
- Người giám sát có thể cấu hình bảo mật dựa trên yêu cầu của chủ sở hữu

Bốn mô hình điều khiển truy cập chính

- Điều khiển truy cập bắt buộc
  - Mandatory Access Control - MAC
- Điều khiển truy cập tùy ý
  - Discretionary Access Control - DAC
- Điều khiển truy cập dựa trên vai trò
  - Role Based Access Control - RBAC
- Điều khiển truy cập dựa trên quy tắc
  - Rule Based Access Control - RBAC

Điều khiển truy cập bắt buộc - MAC

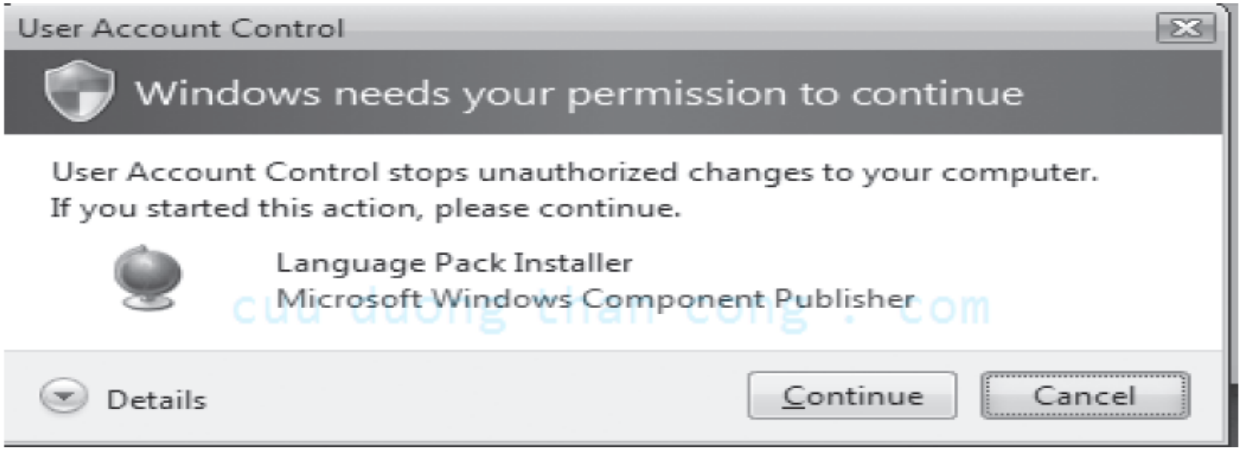
- Điều khiển truy cập bắt buộc
  - Là mô hình điều khiển truy cập nghiêm ngặt nhất
  - Thường bắt gặp trong các thiết lập của quân đội
  - Hai thành phần: Nhãn và Cấp độ
- Mô hình MAC cấp quyền bằng cách đối chiếu nhãn của đối tượng với nhãn của chủ thể
  - Nhãn cho biết cấp độ quyền hạn
- Để xác định có mở một file hay không:
  - So sánh nhãn của đối tượng với nhãn của chủ thể
  - Chủ thể phải có cấp độ tương đương hoặc cao hơn đối tượng được cấp phép truy cập

Điều khiển truy cập bắt buộc – MAC (tiếp)

- Hai mô hình thực thi của MAC
  - Mô hình mạng lưới (Lattice model)
  - Mô hình Bell-LaPadula
- Mô hình mạng lưới
  - Các chủ thể và đối tượng được gán một "cấp bậc" trong mạng lưới
  - Nhiều mạng lưới có thể được đặt cạnh nhau
- Mô hình Bell-LaPadula
  - Tương tự mô hình mạng lưới
  - Các chủ thể không thể tạo một đối tượng mới hay thực hiện một số chức năng nhất định đối với các đối tượng có cấp thấp hơn

Điều khiển truy cập bắt buộc – MAC (tiếp)

- Ví dụ về việc thực thi mô hình MAC
  - Windows 7/Vista có bốn cấp bảo mật
  - Các thao tác cụ thể của một chủ thể đối với phân hạng thấp hơn phải được sự phê duyệt của quản trị viên
- Hộp thoại User Account Control (UAC) trong Windows

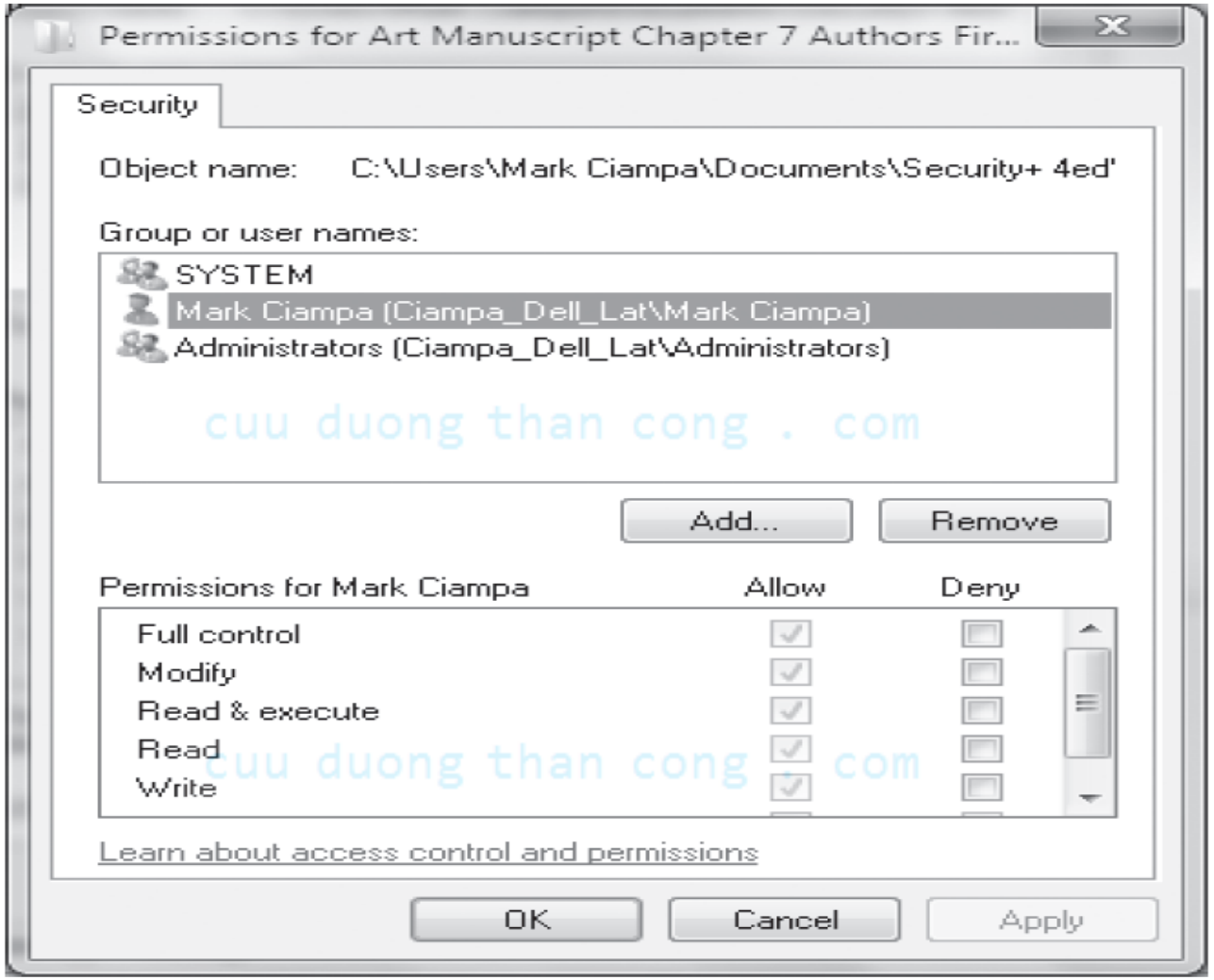


Điều khiển truy cập tùy quyền (DAC)

- Điều khiển truy cập tùy ý (DAC)
  - Mô hình ít hạn chế nhất
  - Mọi đối tượng đều có một chủ sở hữu
  - Chủ sở hữu có toàn quyền điều khiển đối với đối tượng của họ
  - Chủ sở hữu có thể cấp quyền đối với đối tượng của mình cho một chủ thể khác
  - Được sử dụng trên các hệ điều hành như Microsoft Windows và hầu hết các hệ điều hành UNIX

Điều khiển truy cập tùy quyền (DAC) (tiếp)

- Nhược điểm của DAC
  - Phụ thuộc vào quyết định của người dùng để thiết lập cấp độ bảo mật phù hợp
  - Việc cấp quyền có thể không chính xác
  - Quyền của chủ thể sẽ được "thừa kế" bởi các chương trình mà chủ thể thực thi
  - Trojan là một vấn đề đặc biệt của DAC


Permissions for Art Manuscript Chapter 7 Authors Fir...
Security
Object name: C:\Users\Mark Ciampa\Documents\Security+ 4ed'
Group or user names:
SYSTEM
Mark Ciampa (Ciampa_Dell_Lat\Mark Ciampa)
Administrators (Ciampa_Dell_Lat\Administrators)
cuu duong than cong . com
Add...
Remove
Permissions for Mark Ciampa
Allow
Deny
Full control
Modify
Read & execute
Read
Write
cuu duong than cong . com
Learn about access control and permissions
OK
Cancel
Apply

Điều khiển truy cập dựa trên vai trò (RBAC)

- Điều khiển truy cập dựa trên vai trò (Role Based Access Control – RBAC)
  - Còn được gọi là điều khiển truy cập không tùy ý
  - Quyền truy cập dựa trên chức năng công việc
- RBAC gán các quyền cho các vai trò cụ thể trong tổ chức
  - Các vai trò sau đó được gán cho người dùng

Điều khiển truy cập dựa trên quy tắc

- Điều khiển truy cập dựa trên quy tắc (Rule Based Access Control - RBAC)
  - Tự động gán vai trò cho các chủ thể dựa trên một tập quy tắc do người giám sát xác định
  - Mỗi đối tượng tài nguyên chứa các thuộc tính truy cập dựa trên quy tắc
  - Khi người dùng truy cập tới tài nguyên, hệ thống sẽ kiểm tra các quy tắc của đối tượng để xác định quyền truy cập
  - Thường được sử dụng để quản lý truy cập người dùng tới một hoặc nhiều hệ thống
  - Những thay đổi trong doanh nghiệp có thể làm cho việc áp dụng các quy tắc thay đổi

Tóm tắt các mô hình điều khiển truy cập

Tên	Hạn chế	Mô tả
Điều khiển truy cập bắt buộc (MAC)	Người dùng không thể thiết lập điều khiển	Là mô hình nghiêm ngặt nhất
Điều khiển truy cập tùy ý (DAC)	Chủ thể có toàn quyền đối với các đối tượng	Là mô hình cởi mở nhất
Điều khiển truy cập dựa trên vai trò (RBAC)	Gán quyền cho các vai trò cụ thể trong tổ chức,	Được coi là phương pháp thực tế hơn
Điều khiển truy cập dựa trên quy tắc	Tự động gán vai trò cho các chủ thể dựa trên một tập quy tắc do người giám sát xác định	Được sử dụng để quản lý truy cập người dùng tới một hoặc nhiều hệ thống

Thực thi điều khiển truy cập

- Danh sách điều khiển truy cập (Access Control List - ACL)
- Chính sách nhóm (Group Policy)
- Giới hạn tài khoản

Danh sách điều khiển truy cập

- Tập các quyền gắn với một đối tượng
- Xác định chủ thể nào có thể truy cập tới đối tượng và các thao tác nào mà chủ thể có thể thực hiện
- Khi chủ thể yêu cầu thực hiện một thao tác:
  - Hệ thống kiểm tra danh sách điều khiển truy cập đối với mục đã được duyệt
- Danh sách điều khiển truy cập thường được xem xét trong mối liên hệ với các file của hệ điều hành

File chứa quyền truy cập trong Unix

```
$ setfacl -m user:tdk:rw- samplefile
$ getacl samplefile
# file: samplefile
# owner: reo
# group: sysadmin
user::rw-user:
tdk:rw-              #effective:r--
group::r--           #effective:r--
mask:r--
other:r--
```

Danh sách điều khiển truy cập (tiếp)

- Mỗi một mục trong bảng danh sách điều khiển truy cập được gọi là một mục điều khiển (ACE)
- Cấu trúc ACE (trong Windows)
  - Nhận dạng bảo mật (Access identifier) cho tài khoản người dùng hoặc tài khoản nhóm hoặc phiên đăng nhập
  - Mặt nạ truy cập (access mask) xác định quyền truy cập do ACE điều khiển
  - Cờ (Flag) cho biết kiểu của ACE
  - Tập các cờ (Set of flags) xác định đối tượng có thể kế thừa các quyền hay không

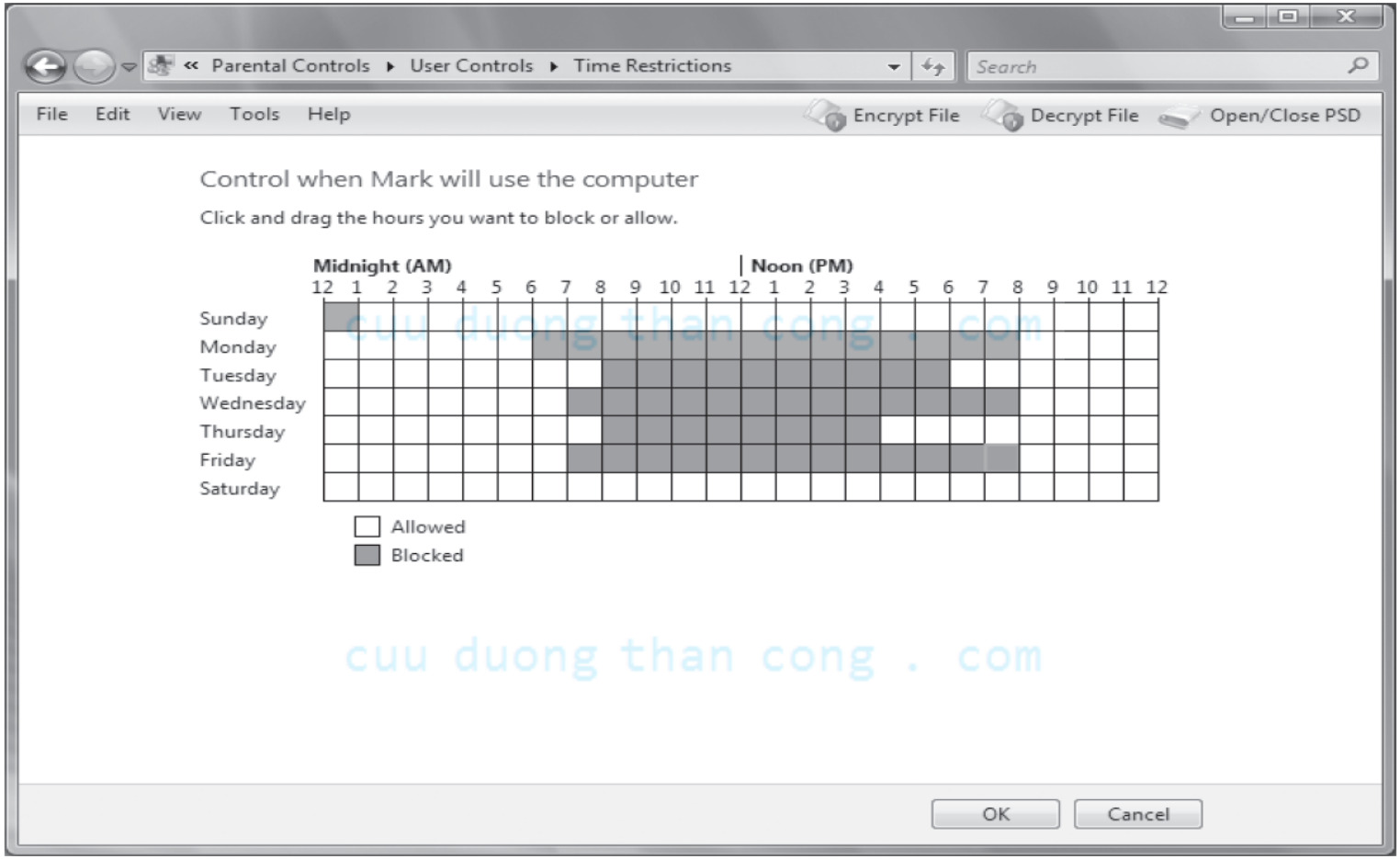
Chính sách nhóm

- Tính năng của Microsoft Windows
  - Cho phép sử dụng Active Directory (AD) để quản lý và cấu hình tập trung cho các máy tính và người dùng từ xa
  - Thường được sử dụng trong các môi trường doanh nghiệp
  - Các thiết lập được lưu trữ trong các GPO (Group Policy Objects – Đối tượng chính sách nhóm)
- Local Group Policy
  - Có ít tùy chọn hơn so với Group Policy
  - Được sử dụng để cấu hình các thiết lập cho các hệ thống không phải là một phần của AD

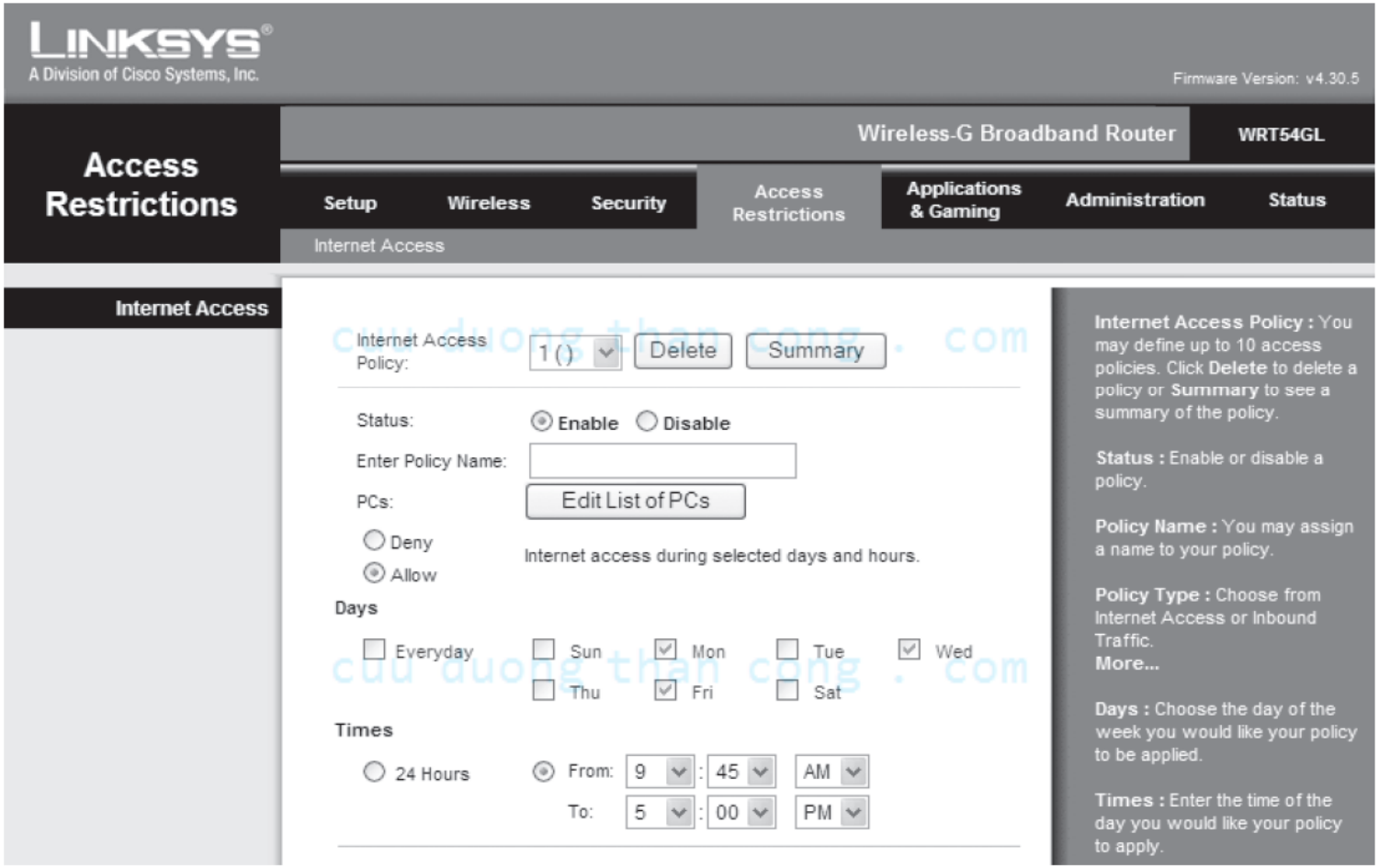
Giới hạn tài khoản

- Giới hạn thời gian trong ngày (time of day restriction)
  - Giới hạn số lần người dùng đăng nhập vào hệ thống trong một ngày
  - Cho phép chọn khối thời gian chặn đối với các truy cập được cho phép
  - Có thể được thiết lập trên từng hệ thống riêng lẻ
- Hạn sử dụng tài khoản (account expiration)
  - Các tài khoản "mồ côi" (orphaned account): tài khoản vẫn còn hoạt động sau khi một nhân viên rời khỏi tổ chức
  - Tài khoản không hoạt động (dormant account): không truy cập trong một khoảng thời gian dài
  - Cả hai kiểu tài khoản trên là những nguy cơ đối với bảo mật

Giới hạn thời gian trong ngày của hệ điều hành



Giới hạn đối với điểm truy cập không dây



Giới hạn tài khoản (tiếp)

- Các khuyến cáo xử lý đối với tài khoản "mồ côi" và tài khoản "ngủ đông"
  - Thiết lập một qui trình chính thức
  - Chấm dứt truy cập ngay lập tức
  - Quản lý nhật ký (file log)
- Các tài khoản "mồ côi" vẫn là một vấn đề nan giải đối các tổ chức hiện nay
- Account expiration (thời gian hiệu lực của tài khoản)
  - Thiết lập hết hạn cho một tài khoản người dùng (hết hiệu lực)

Giới hạn tài khoản (tiếp)

- Password expiration (thời gian hiệu lực của mật khẩu) thiết lập khoảng thời gian mà người dùng phải thay đổi một mật khẩu mới
  - Khác với account expiration (thời gian hiệu lực của tài khoản)
- Account expiration có thể được thiết lập bằng số ngày mà người dùng không có bất cứ hành động truy cập nào

1.3. Các công nghệ xác thực và nhận dạng người dùng

Các đặc điểm của điều khiển truy cập

Loại điều khiển truy cập	Giải pháp
Sinh trắc học	• Tĩnh: vân tay, mống mắt, mặt, bàn tay • Động: tiếng nói, gõ bàn phím, các chuyển động, cử chỉ
Token	• Đồng bộ hoặc bất đồng bộ • Smart card hoặc memory card
Mật khẩu	• Kiểm soát mật khẩu nghiêm ngặt đối với người dùng • Các chính sách khóa tài khoản • Kiểm tra các sự kiện đăng nhập
Single sign-on	• Quy trình Keberos • …

Các dịch vụ xác thực

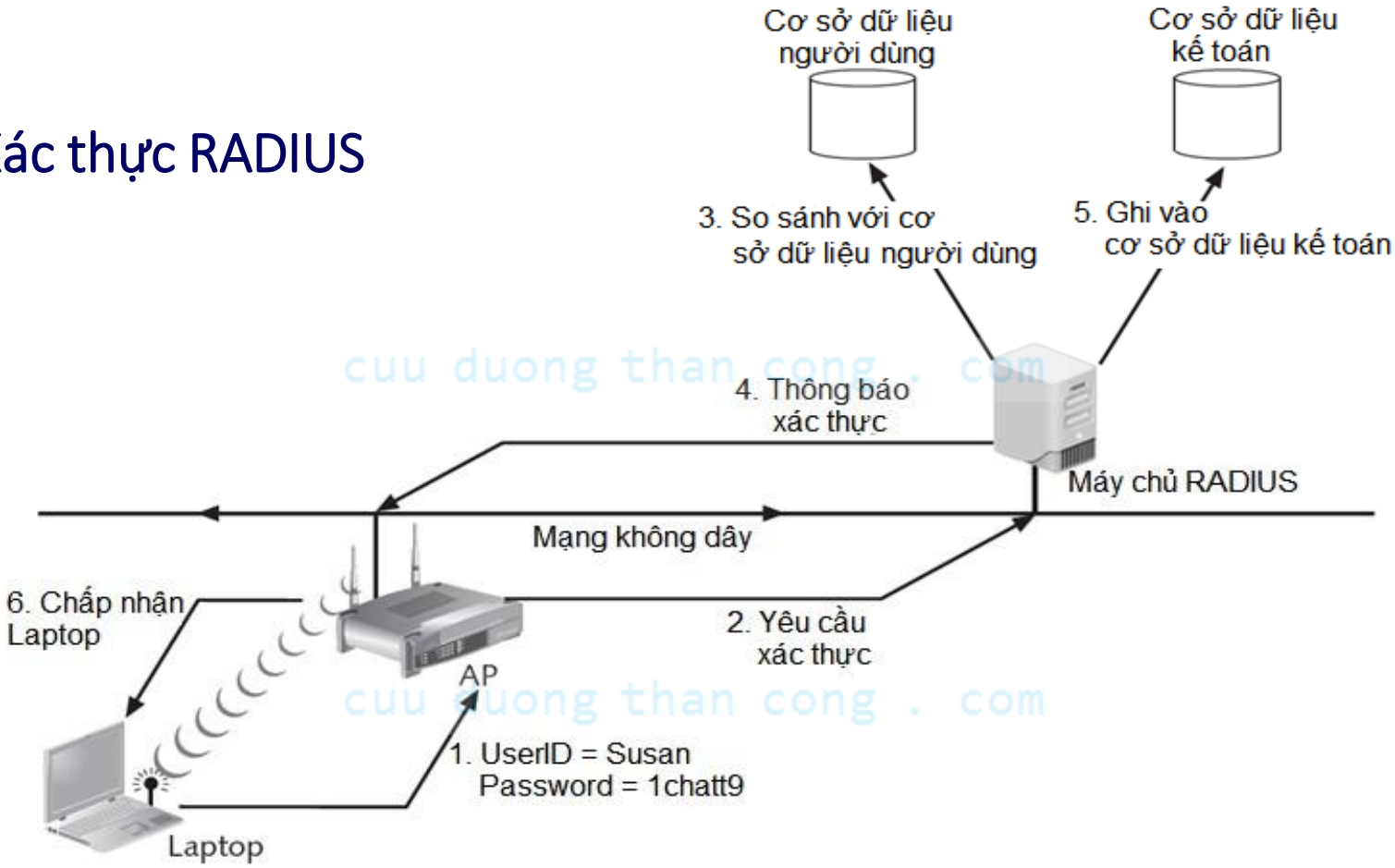
- Xác thực (Authentication): Quá trình xác minh thông tin
- Các dịch vụ xác thực được cung cấp trên một mạng
  - Máy chủ xác thực chuyên dụng
    - Còn gọi là máy chủ AAA nếu nó thực hiện đồng thời cả nhiệm vụ ủy quyền (authorization) và kế toán (accounting)
- Các kiểu xác thực và máy chủ AAA thông dụng
  - RADIUS
  - Kerberos
  - TACACS
  - LDAP

RADIUS

- RADIUS (Remote Authentication Dial In User Service - Bộ quay số xác thực từ xa trong dịch vụ người dùng)
  - Được giới thiệu vào năm 1992
  - Trở thành một tiêu chuẩn công nghiệp
  - Phù hợp cho các ứng dụng kiểm soát dịch vụ cỡ lớn
    - Ví dụ như truy cập quay số tới mạng doanh nghiệp
  - Hiện nay xẫn đang được sử dụng
- RADIUS client
  - Thường là một thiết bị như điểm truy cập không dây (AP)
    - Có nhiệm vụ gửi các thông tin về người dùng cùng với các tham số kết nối tới máy chủ RADIUS

RADIUS (tiếp)

Xác thực RADIUS



RADIUS (tiếp)

- Hồ sơ người dùng RADIUS được lưu trữ trong cơ sở dữ liệu trung tâm
  - Tất cả các máy chủ từ xa đều có thể chia sẻ thông tin
- Ưu điểm của dịch vụ trung tâm
  - Tăng cường bảo mật do chỉ có duy nhất một điểm quản lý trên mạng
  - Dễ dàng theo dõi và truy vết việc sử dụng để thanh toán và lưu giữ các số liệu thống kê mạng

LDAP

- LDAP (Lightweight Directory Access Control - Giao thức truy cập thư mục hạng nhẹ)
- Dịch vụ thư mục
  - Cơ sở dữ liệu được lưu trên mạng
  - Chứa các thông tin về người dùng và các thiết bị mạng
  - Lưu vết theo dõi các tài nguyên mạng và đặc quyền của
  - người dùng đối với những tài nguyên đó
  - Cho phép hoặc từ chối truy cập dựa trên thông tin lưu trữ
- Tiêu chuẩn cho các dịch vụ thư mục
  - X.500
  - DAP (Directory Access Protocol - Giao thức truy cập thư mục)

LDAP (tiếp)

- LDAP
  - Một tập con đơn giản hơn của DAP
  - Được thiết kế để hoạt động trên bộ giao thức TCP/IP
  - Có các chức năng đơn giản hơn
  - Mã hóa các thành phần giao thức theo cách đơn giản hơn so với X.500
  - Là một giao thức mở
- Nhược điểm của LDAP
  - Có thể là mục tiêu của tấn công tiêm nhiễm LDAP
  - Tương tự như tấn công tiêm nhiễm SQL
  - Xảy ra khi dữ liệu do người dùng cung cấp không được lọc đúng cách

2. Tường lửa

2. Tường lửa

1. Khái niệm
2. Chế độ xử lý của tường lửa
3. Phân loại
4. Lựa chọn, cấu hình tường lửa
5. Lọc nội dung

2.1. Khái niệm tường lửa

- Ngăn chặn các thông tin cụ thể từ di chuyển từ vùng bên ngoài (mạng không tin cậy) đến vùng bên trong (mạng tin cậy) của hệ thống thông tin và ngược lại
- Có thể là hệ thống máy tính riêng biệt; hay một dịch vụ phần mềm chạy trên router hoặc máy chủ hiện có; hoặc một mạng riêng biệt chứa các thiết bị hỗ trợ

2.2. Các chế độ xử lý của tường lửa

- Năm chế độ xử lý của tường lửa:
  - Lọc gói tin
  - Gateway ứng dụng
  - Gateway mức mạng (circuit)
  - Tường lửa lớp MAC
  - Lai

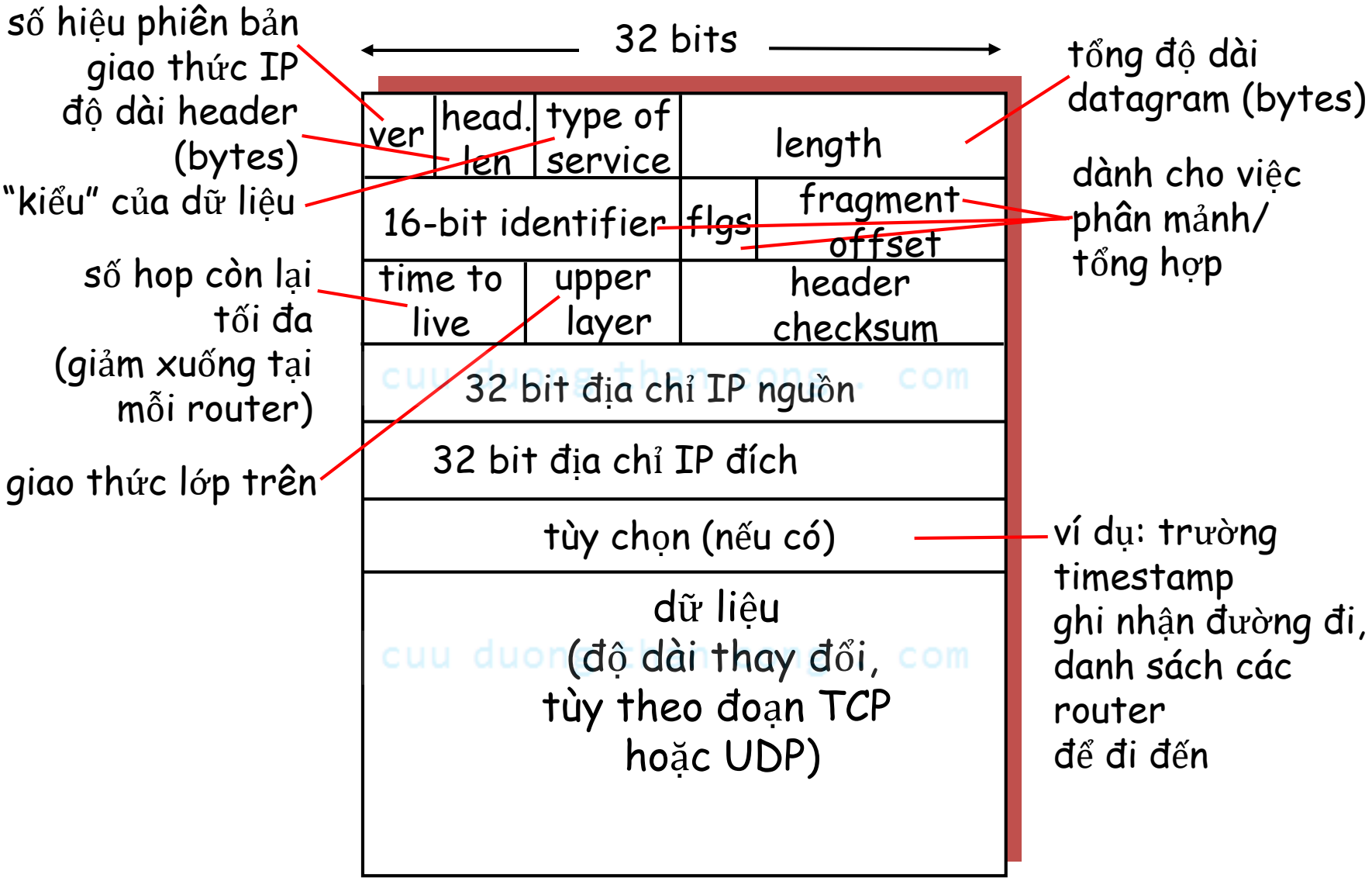
Lọc gói tin

- Tường lửa lọc gói tin kiểm tra các thông tin header của gói dữ liệu
- Thường dựa trên sự kết hợp của:
  - Địa chỉ IP nguồn và đích
  - Hướng (vào trong hay ra ngoài)
  - Các yêu cầu cổng nguồn và đích TCP hay UDP
- Mô hình tường lửa đơn giản thực thi các quy tắc được thiết kế để ngăn chặn các gói tin với các địa chỉ rõ ràng hoặc một phần địa chỉ

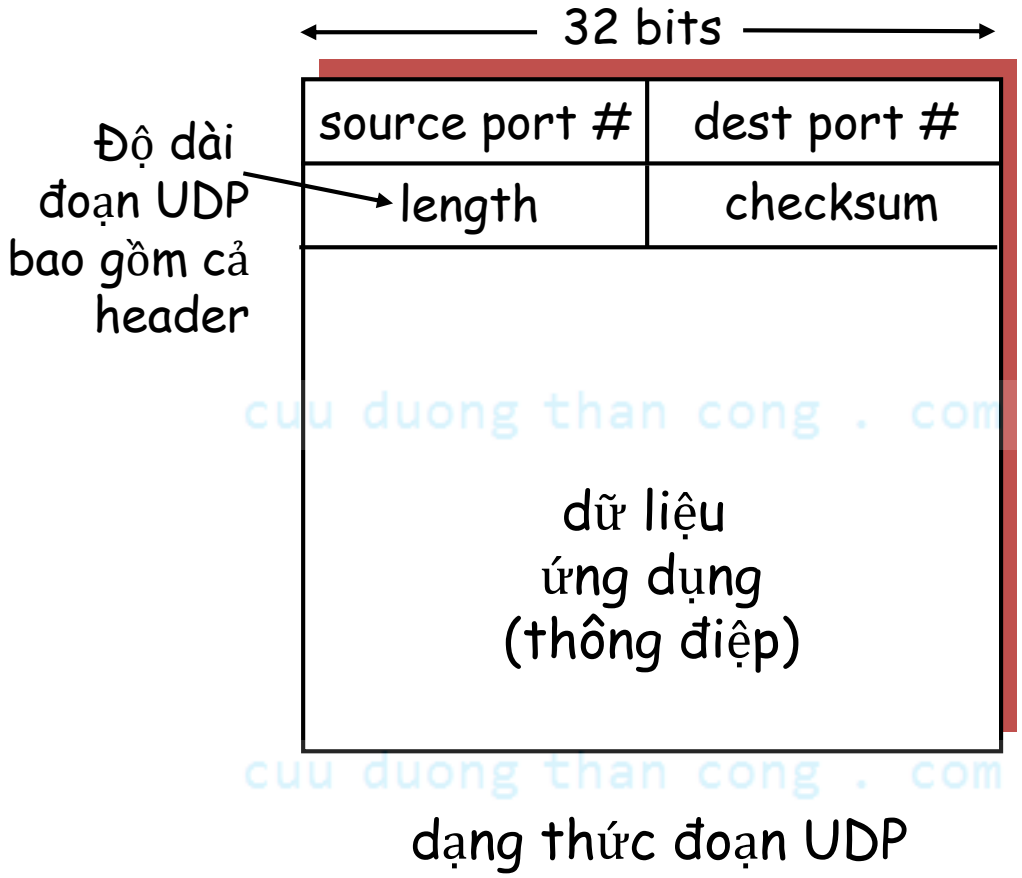
Lọc gói tin (tiếp)

- Có 3 loại tường lửa lọc gói tin:
  - Lọc tĩnh: các luật lọc sẽ điều khiển cách thức mà tường lửa quyết định các gói tin được phép và bị từ chối
  - Lọc động: cho phép tường lửa phản ứng với sự kiện xuất hiện và cập nhật hoặc tạo ra các quy tắc để đối phó với các sự kiện
  - Kiểm tra có trạng thái: tường lửa theo dõi các kết nối mạng giữa các hệ thống nội bộ và bên ngoài bằng cách sử dụng một bảng trạng thái

Định dạng IP datagram

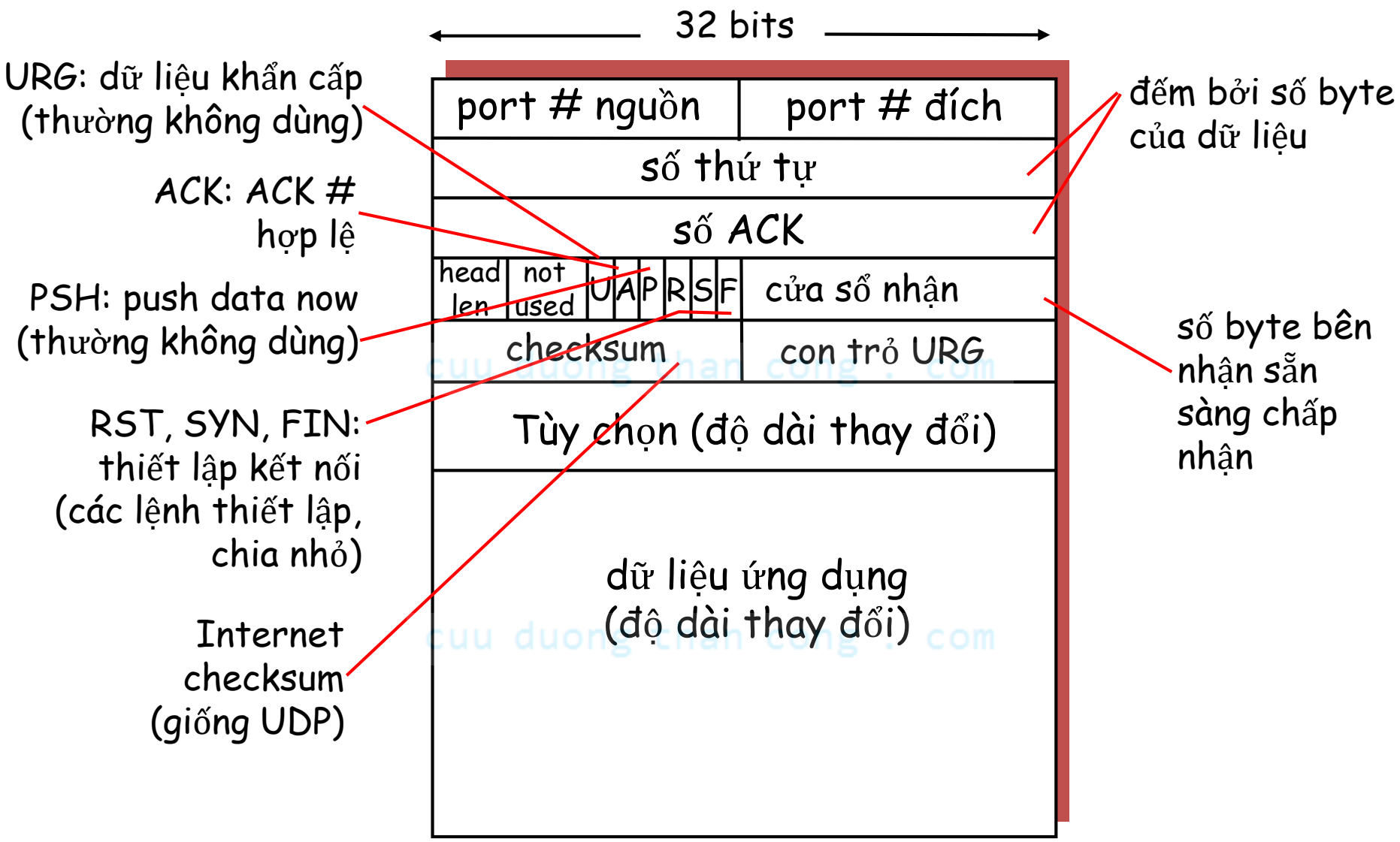


Định dạng UDP segment

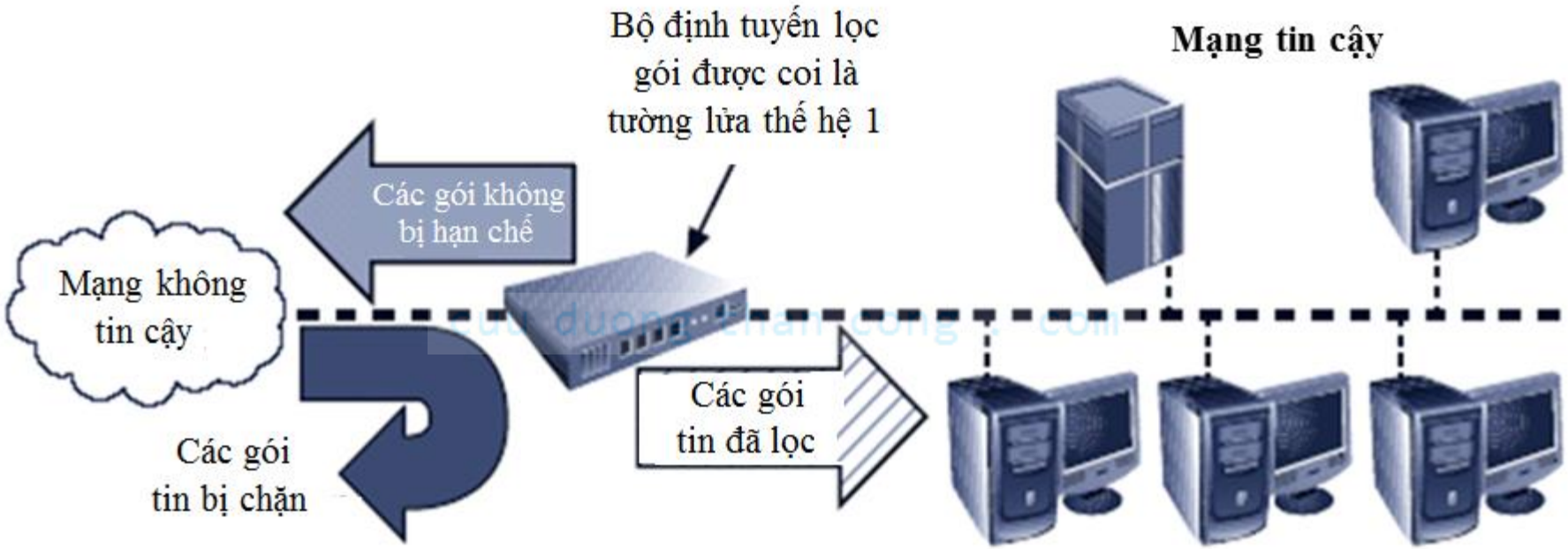


dạng thức đoạn UDP

Định dạng TCP segment



Bộ định tuyến lọc gói tin



Ví dụ về định dạng và luật của tường lửa

Địa chỉ nguồn	Địa chỉ đích	Dịch vụ (HTTP, FTP, SMTP,…)	Hành động (Cho phép / từ chối)
172.16.x.x	10.10.x.x	Bất kỳ	Từ chối
192.168.x.x	10.10.10.25	HTTP	Cho phép
192.168.0.1	10.10.10.10	FTP	Cho phép

Gateway ứng dụng

- Thường được cài đặt trên một máy tính chuyên dụng; cũng được biết đến như là một máy chủ proxy
- Máy chủ proxy thường được đặt trong khu vực không được đảm bảo an toàn của mạng (ví dụ, DMZ), nó có nhiều rủi ro hơn đến từ các nguy cơ từ mạng ít tin cậy
- Bộ định tuyến lọc bổ sung có thể được cài đặt phía sau máy chủ proxy, để bảo vệ các hệ thống nội bộ tốt hơn
- Có hiệu quả cao nhất trong tất cả các loại tường lửa

Gateway mức mạng

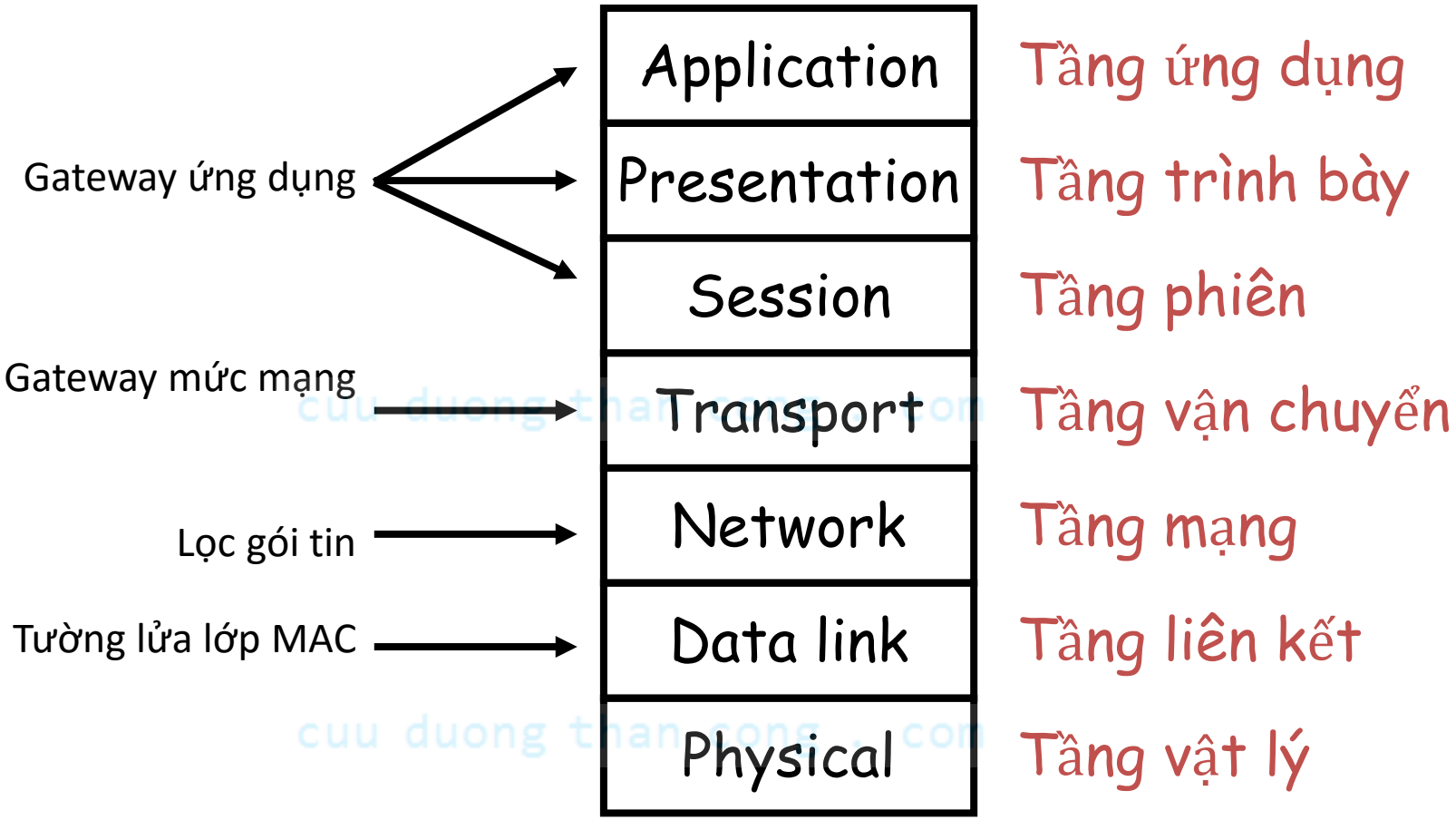
- Tường lửa gateway mức mạng hoạt động ở lớp truyền vận
- Giống như tường lửa lọc gói, thường không nhìn vào lưu lượng dữ liệu truyền tải giữa hai mạng, mà ngăn chặn các kết nối trực tiếp giữa một mạng và một đầu cuối khác
- Thực hiện bằng cách tạo ra các đường hầm kết nối các tiến trình hoặc các hệ thống cụ thể cho mỗi phía của tường lửa, và chỉ cho phép các lưu lượng hợp lệ trong đường hầm

Tường lửa lớp MAC

- Được thiết kế để hoạt động ở lớp điều khiển truy cập của mô hình mạng OSI
- Có thể xem xét định danh của các máy tính cụ thể trong các quyết định lọc

- Địa chỉ MAC của từng máy tính được liên kết tới ACL, xác định cụ thể các loại gói dữ liệu có thể được gửi tới từng máy; tất cả lưu lượng khác sẽ bị chặn

Các kiểu tường lửa và mô hình OSI



Tường lửa lai

- Kết hợp các tính năng của các loại tường lửa; tức là, các tính năng của lọc gói và dịch vụ proxy, hoặc lọc gói và gateway mức mạng
- Hay là, có thể bao gồm hai thiết bị tường lửa riêng biệt; mỗi một hệ thống tường lửa riêng rẽ nhau, nhưng kết nối với nhau để thực hiện công việc song song

2.3. Phân loại tường lửa (theo cấu trúc)

- Hầu hết các tường lửa là các thiết bị: các hệ thống độc lập, đầy đủ
- Hệ thống tường lửa thương mại bao gồm các phần mềm ứng dụng tường lửa chạy trên máy tính phổ thông
- Tường lửa cho văn phòng nhỏ/văn phòng tại nhà (SOHO) hoặc cho cá nhân (được biết đến như gateway băng thông rộng hoặc router DSL/modem cáp) kết nối mạng nội bộ của người dùng hoặc một hệ thống máy tính cụ thể tới thiết bị kết nối Internet
- Phần mềm tường lửa cá nhân được cài đặt trực tiếp trên hệ thống của người dùng

Tường lửa SOHO: phần mềm hay phần cứng

- Người dùng cá nhân nên cài đặt tường lửa loại nào?
- Nơi nào cần bảo vệ để chống lại hacker?
- Với tùy chọn phần mềm, hacker là bên trong máy tính của bạn

- Với thiết bị phần cứng, ngay cả khi hacker phá vỡ hệ thống tường lửa, máy tính và thông tin vẫn an toàn phía sau kết nối đã chặn

Kiến trúc của tường lửa

- Thiết bị tường lửa có thể được cấu hình theo một số kiến trúc kết nối mạng
- Cấu hình hoạt động tốt nhất phụ thuộc vào ba yếu tố:
  - Mục tiêu của mạng
  - Khả năng của tổ chức trong việc xây dựng và thực hiện các kiến trúc
  - Ngân sách dành cho hoạt động
- Bốn kiểu cài đặt theo kiến trúc phổ biến của tường lửa: bộ định tuyến lọc gói, tường lửa screened host, tường lửa dual-homed, tường lửa screened subnet

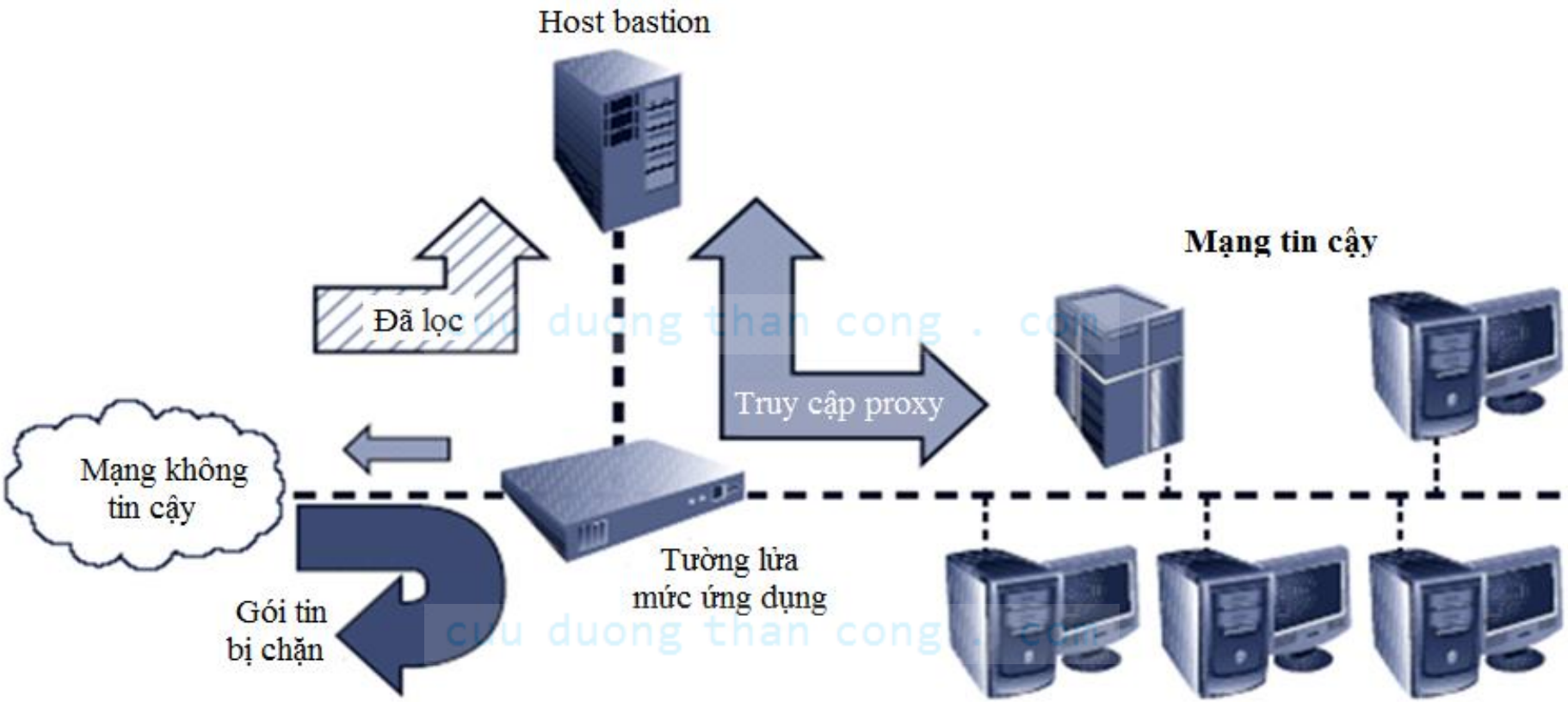
Bộ định tuyến lọc gói tin

- Hầu hết các tổ chức có kết nối Internet sẽ có một router phục vụ làm giao diện tới Internet
- Đa phần các thiết bị định tuyến có thể được cấu hình để từ chối các gói tin không cho phép vào mạng
- Nhược điểm là thiếu kiểm định và thiếu phương pháp xác thực mạnh

Bộ định tuyến lọc gói tin (tiếp)

Tường lửa Screened Host

- Kết hợp lọc gói tin router với tường lửa chuyên dụng riêng, ví dụ như máy chủ proxy ứng dụng
- Cho phép router chọn lựa gói dữ liệu để giảm thiểu lưu lượng và tải về proxy nội bộ
- Host riêng biệt thường được gọi tắt là bastion host (pháo đài); có thể là mục tiêu tốt cho các cuộc tấn công từ bên ngoài và cần được bảo vệ rất kỹ lưỡng

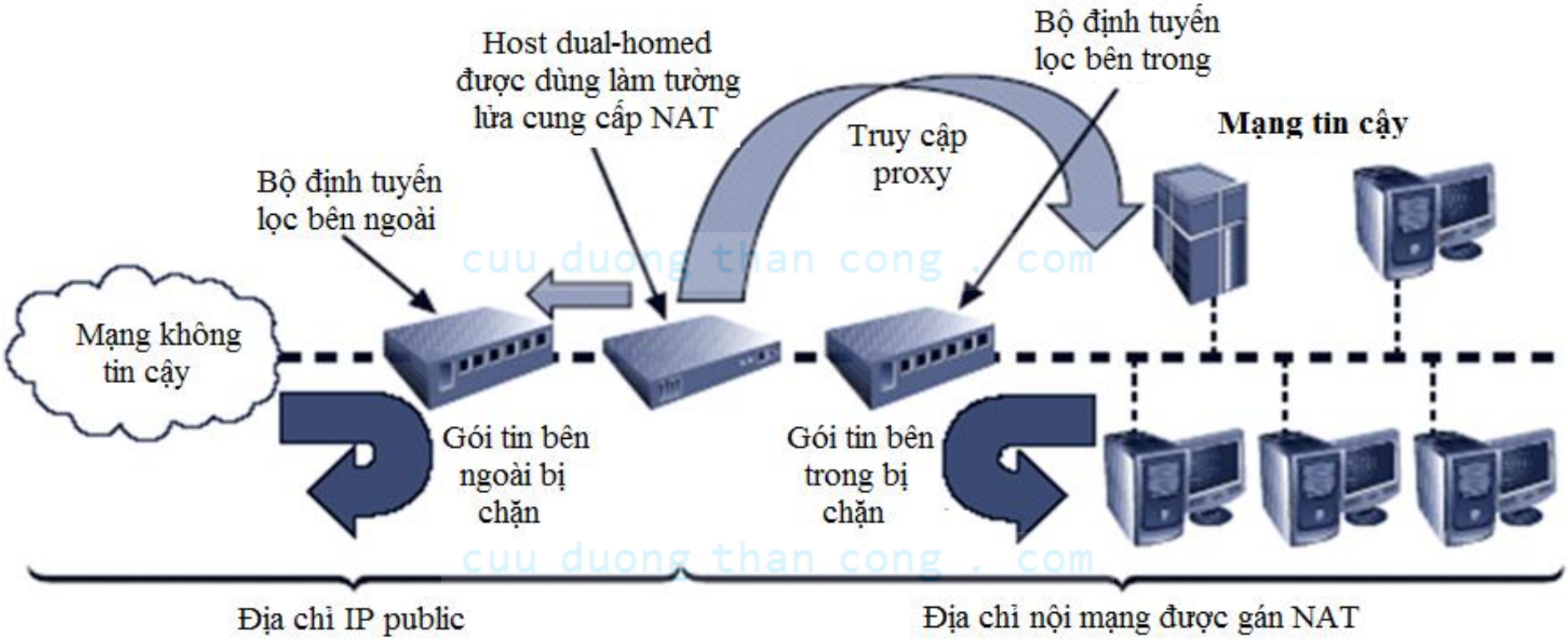


Tường lửa Dual-Homed Host

- Bastion host có hai card giao diện mạng (NIC): một kết nối với mạng bên ngoài, một kết nối với mạng nội bộ
- Khi thực hiện các kiến trúc này, người ta thường sử dụng NAT, tạo ra một rào cản đối với sự xâm nhập từ bên ngoài

Dải địa chỉ dự trữ không thể định tuyến

Class (Lớp)	Từ	Tới	Mặt nạ CIDR	Mặt nạ thập phân
Class "A" or 24 Bit	10.0.0.0	10.255.255.255	/8	255.0.0.0
Class "B" or 20 Bit	172.16.0.0	172.31.255.255	/12 or /16	255.240.0.0 or 255.255.0.0
Class "C" or 16 Bit	192.168.0.0	192.168.255.255	/16 or /24	255.255.0.0 or 255.255.255.0

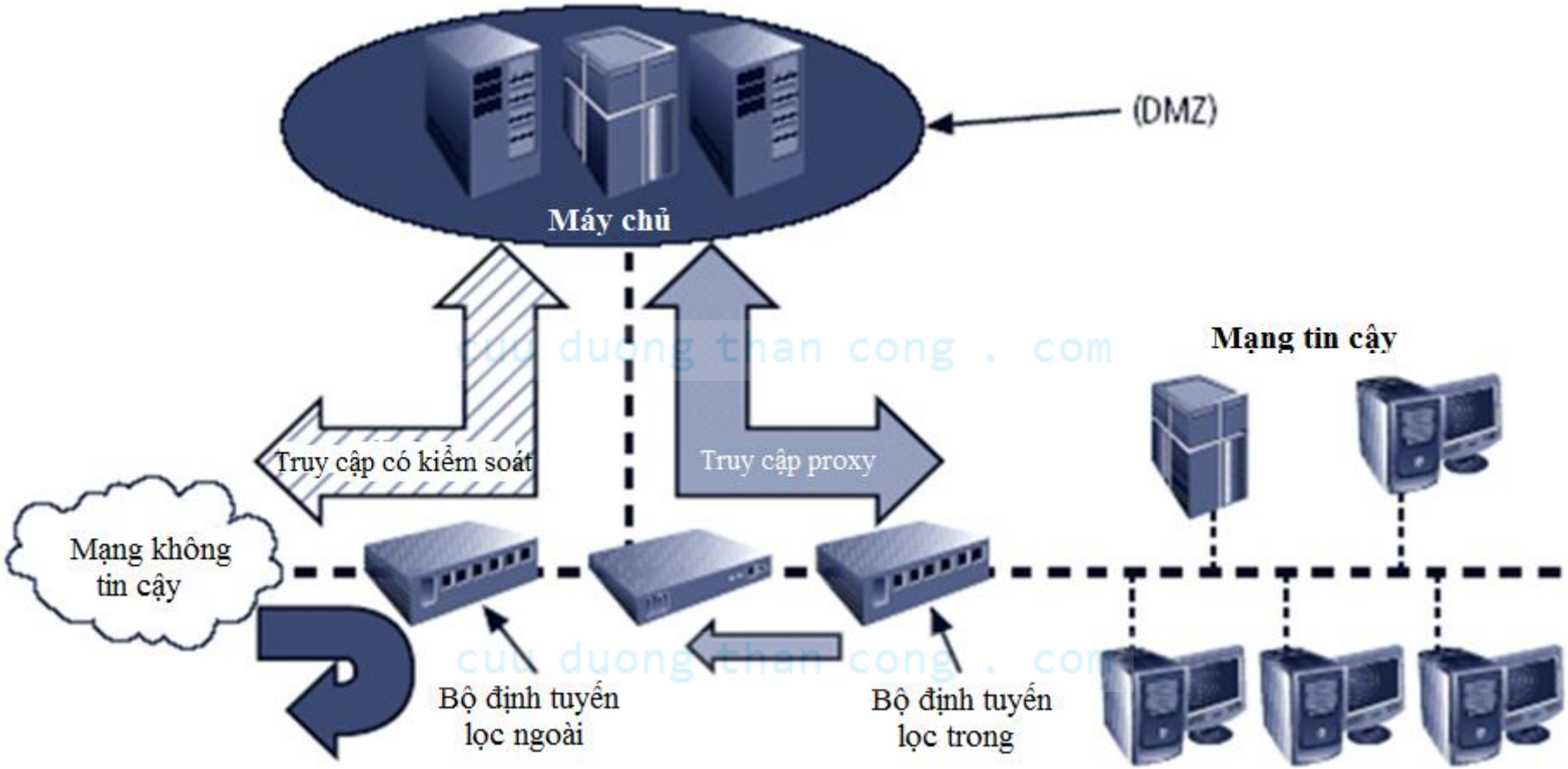


Tường lửa Screened Subnet (với DMZ)

- Kiến trúc chủ yếu được sử dụng hiện nay là các tường lửa Screened Subnet
- Thường bao gồm hai hoặc nhiều bastion host nội bộ, nằm phía sau router lọc gói, với mỗi host bảo vệ mạng tin cậy:
  - Kết nối từ bên ngoài (mạng không tin cậy) được định tuyến thông qua router lọc gói phía ngoài
  - Kết nối từ bên ngoài (mạng không tin cậy) được định tuyến vào và ra tường lửa định tuyến, nhằm tách phân đoạn mạng (được gọi là DMZ)
  - Kết nối vào mạng nội bộ tin cậy được phép chỉ khi xuất phát ttừ các máy chủ DMZ bastion host

Tường lửa Screened Subnet (với DMZ) (tiếp)

- Screened Subnet thực hiện hai chức năng:
  - Bảo vệ hệ thống DMZ và thông tin khỏi các mối đe dọa bên ngoài
  - Bảo vệ mạng nội bộ bằng cách giới hạn cách thức kết nối bên ngoài có thể truy cập vào hệ thống nội bộ
- Một khía cạnh khác của DMZ: Extranet



2.4. Lựa chọn đúng tường lửa

- Khi lựa chọn tường lửa, hãy xem xét một số yếu tố:
  - Tường lửa nào cung cấp sự cân bằng giữa khả năng bảo vệ và chi phí cho các nhu cầu của tổ chức?
  - Những tính năng được bao gồm trong giá cơ sở?
  - Có dễ cài đặt và cấu hình? Khả năng truy cập của kỹ thuật nhân viên khi cấu hình tường lửa?
  - Tường lửa có thể thích nghi với sự phát triển của mạng máy tính trong tổ chức?
- Vấn đề quan trọng thứ hai là chi phí

Cấu hình và quản lý tường lửa

- Mỗi thiết bị tường lửa phải có tập các quy tắc cấu hình riêng của mình để điều chỉnh các hành động của nó
- Cấu hình chính sách tường lửa thường phức tạp và khó khăn
- Việc cấu hình chính sách cho tường lửa là cả một nghệ thuật và khoa học
- Khi quy tắc an toàn xung đột với hiệu suất kinh doanh, an toàn thường bị loại bỏ

Các kinh nghiệm thực tiễn với tường lửa

- Tất cả lưu lượng truy cập từ mạng tin cậy được phép đi ra ngoài
- Thiết bị tường lửa không bao giờ được truy cập trực tiếp từ mạng công cộng
- Dữ liệu SMTP được phép đi qua tường lửa
- Dữ liệu ICMP bị từ chối
- Truy cập Telnet đến máy chủ nội bộ nên bị chặn
- Khi các dịch vụ Web được cung cấp ra ngoài bức tường thì cần từ chối các lưu lượng HTTP muốn vào các mạng nội bộ

Các quy tắc cho tường lửa

- Hoạt động bằng cách kiểm tra các gói dữ liệu và thực hiện so sánh với các quy tắc logic định trước
- Logic dựa vào tập các nguyên tắc phổ biến nhất được gọi là quy tắc tường lửa, cơ sở quy tắc, hoặc logic tường lửa
- Hầu hết các tường lửa sử dụng thông tin header của gói tin để xác định xem liệu một gói tin cụ thể có được cho phép hay từ chối

Ví dụ về chính sách cho tường lửa

- Loại tất cả các được định tuyến theo nguồn bởi vì định tuyến theo nguồn có thể được sử dụng cho giả mạo địa chỉ .
- Loại các gói tin nếu chúng thông báo là đến từ mạng nội bộ,.
- Cho qua các gói tin khi chúng là một phần của kết nối TCP đã thành lập mà không cần kiểm tra them
- Chặn tất cả các kết nối đến cổng có số hiệu thấp trừ SMTP và DNS.
- Chặn tất cả các dịch vụ lắng nghe các kết nối TCP trên cổng số hiệu cao.
- Kiểm tra các kết nối đến từ cổng 20 vào cổng số hiệu cao; chúng được coi là các kết nối dữ liệu FTP.
- Hạn chế truy cập vào chính router (Telnet & SNMP) với access-list 2.
- Chặn tất cả lưu lượng UDP để bảo vệ các dịch vụ RPC.

Cổng và giao thức phổ biến

Cổng	Giao thức
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)

Một vài tập luật

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
10.10.10.0	Any	Any	Any	Allow

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
Any	Any	10.10.10.6	25	Allow

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
10.10.10.0	Any	Any	7	Allow
Any	Any	10.10.10.0	7	Deny

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
10.10.10.0	Any	10.10.10.0	23	Allow
Any	Any	10.10.10.0	23	Deny

Một vài tập luật (tiếp)

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
Any	Any	10.10.10.4	80	Allow

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
Any	Any	10.10.10.5	80	Allow

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
10.10.10.5	80	192.168.2.4	80	Allow

Địa chỉ nguồn	Cổng nguồn	Địa chỉ đích	Cổng đích	Hành động
Any	Any	Any	Any	Deny

2.5. Các bộ lọc nội dung

- Bộ lọc phần mềm – không phải tường lửa - cho phép các quản trị viên hạn chế quyền truy cập nội dung từ bên trong mạng
- Về bản chất, đó là một tập hợp các script hoặc chương trình hạn chế người dùng truy cập vào các giao thức mạng / địa chỉ Internet nhất định
- Trọng tâm chính là để hạn chế truy cập nội bộ tới nội dung bên ngoài
- Hầu hết các bộ lọc nội dung phổ biến hạn chế người dùng truy cập các trang web không phải thương mại hoặc từ chối kết nối đến

3. VPN

3. VPN

1. Khái niệm
2. Các chế độ của VPN

Bảo vệ kết nối từ xa

- Việc cài đặt các kết nối liên mạng yêu cầu đường dây thuê riêng (leased lines) hoặc các kênh dữ liệu khác; những kết nối này thường được đảm bảo theo yêu cầu thỏa thuận dịch vụ chính thức
- Khi các cá nhân tìm cách kết nối với mạng lưới của tổ chức, thì cần phải cung cấp tùy chọn linh hoạt hơn.
- Tùy chọn như mạng riêng ảo (VPN) đã trở nên phổ biến hơn do sự lan truyền của mạng Internet

Mạng riêng ảo (VPN)

- Kết nối mạng riêng và bảo mật giữa các hệ thống; sử dụng khả năng truyền dữ liệu của mạng công cộng và không được bảo mật
- Mở rộng bảo mật các kết nối mạng nội bộ của tổ chức đến các điểm ở xa vượt ra ngoài mạng tin cậy.
- Ba công nghệ VPN được định nghĩa:
  - VPN tin cậy (Trusted VPN)
  - VPN bảo mật (Secure VPN)
  - Lai VPN (kết hợp hai loại trên)

Mạng riêng ảo (VPN) (tiếp)

- VPN phải thực hiện:
  - Đóng gói dữ liệu vào và ra
  - Mã hóa dữ liệu vào và ra
  - Xác thực máy tính ở xa cũng như người dùng ở xa (có thể).

Chế độ truyền tải

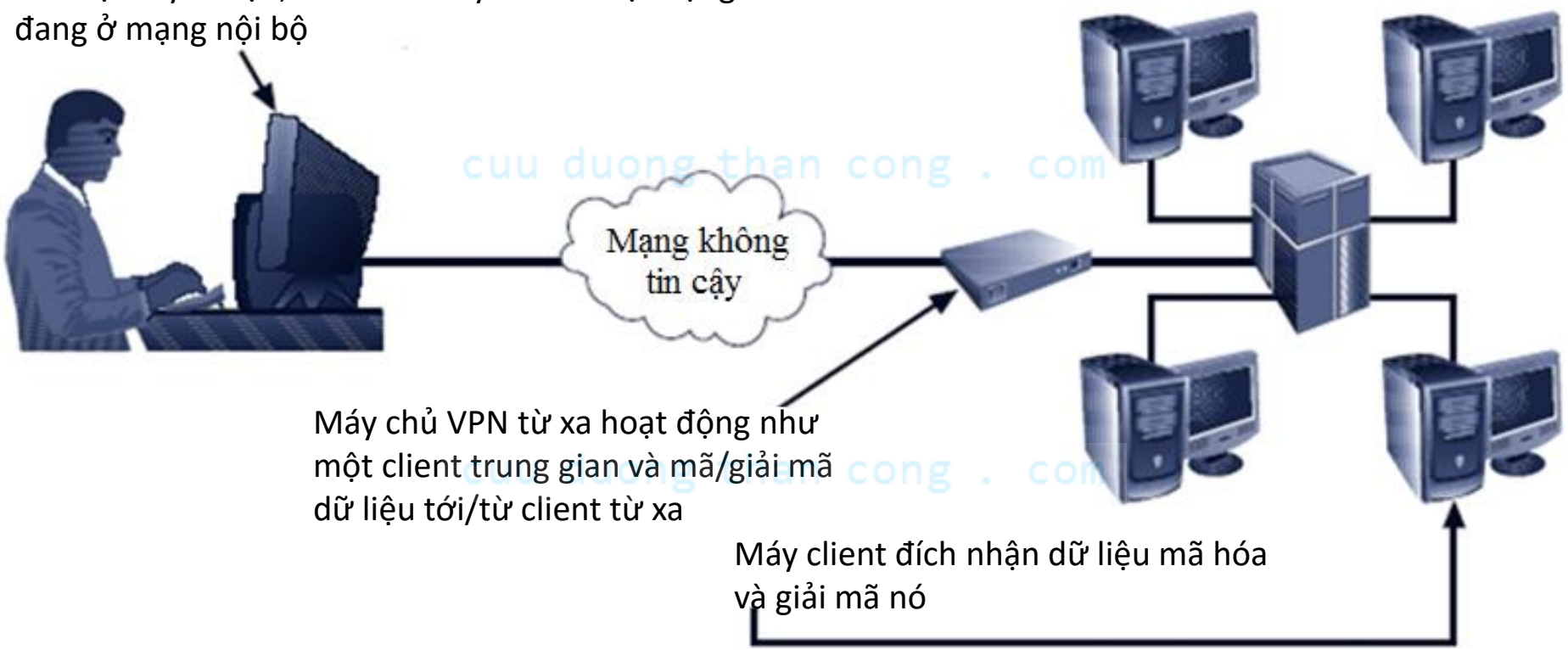
- Dữ liệu trong gói tin IP được mã hóa, nhưng thông tin phần tiêu đề (header) thì không.
- Cho phép người dùng thiết lập liên kết bảo mật trực tiếp đến host ở xa, chỉ mã hóa nội dung dữ liệu của gói tin
- Hai cách sử dụng phổ biến:
  - Truyền tải end-to-end dữ liệu đã mã hóa
  - Nhân viên truy cập từ xa kết nối với mạng lưới văn phòng qua mạng Internet bằng cách kết nối đến một máy chủ VPN trong mạng

VPN ở chế độ truyền tải

Máy client từ xa mã hóa dữ liệu và gửi chúng tới hệ thống đích mà không mã hóa phần tiêu đề

HOẶC

Máy client từ xa yêu cầu kết nối intranet sử dụng VPN chế độ truyền vận, và khi đí máy client hoạt động như đang ở mạng nội bộ



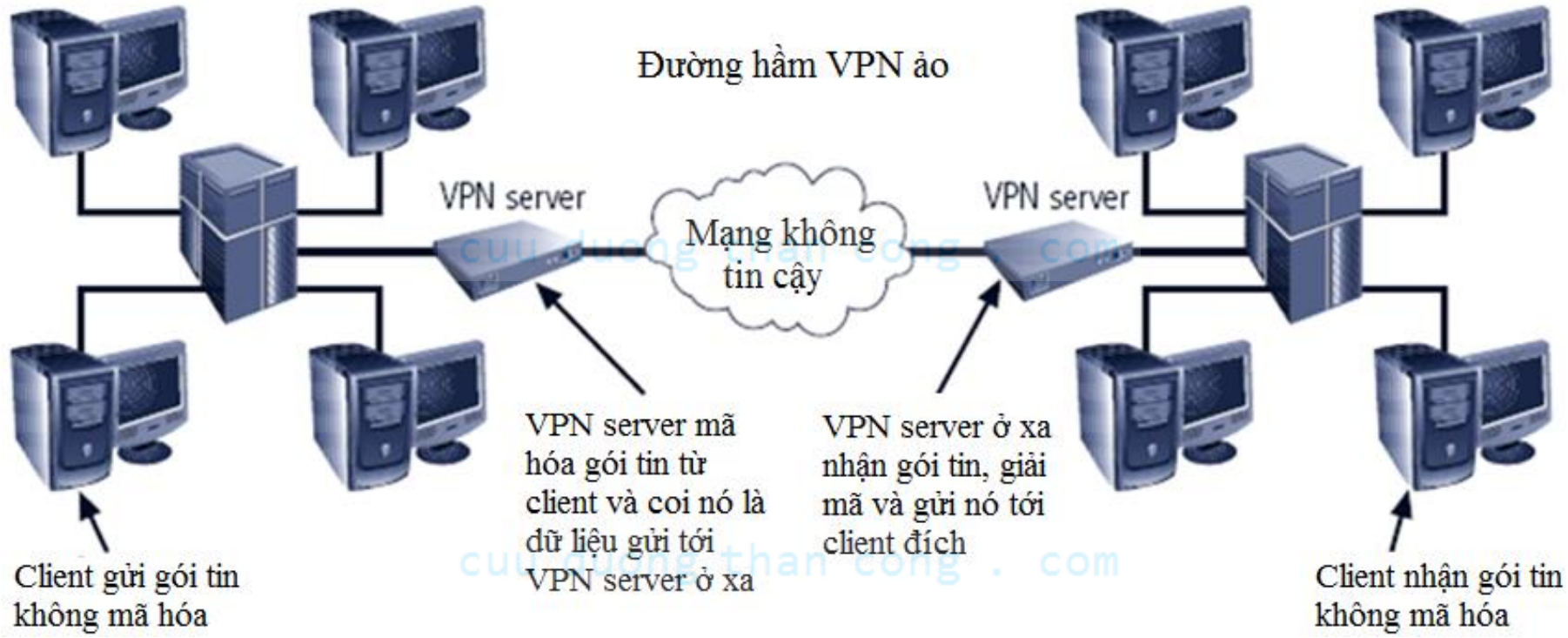
Máy chủ VPN từ xa hoạt động như một client trung gian và mã/giải mã dữ liệu tới/từ client từ xa

Máy client đích nhận dữ liệu mã hóa và giải mã nó

Chế độ đường hầm (Tunnel Mode)

- Tổ chức thiết lập hai máy chủ đường hầm trong mạng
- Các máy chủ này hoạt động có chức năng là điểm mã hóa, mã hóa tất cả lưu lượng đi qua mạng không an toàn
- Lợi ích đầu tiên đối với mô hình này là một gói tin bị chặn sẽ không tiết lộ gì về hệ thống thực
- Ví dụ về VPN chế độ đường hầm: Microsoft's Internet Security and Acceleration (ISA) Server

VPN ở chế độ đường hầm



4. IDS và IPS

4. IDS và IPS

1. Giới thiệu
2. Phân loại
3. Phương pháp phát hiện tấn công
4. Các hành vi đáp trả
5. Lựa chọn IDS và IPS
6. Triển khai cài đặt

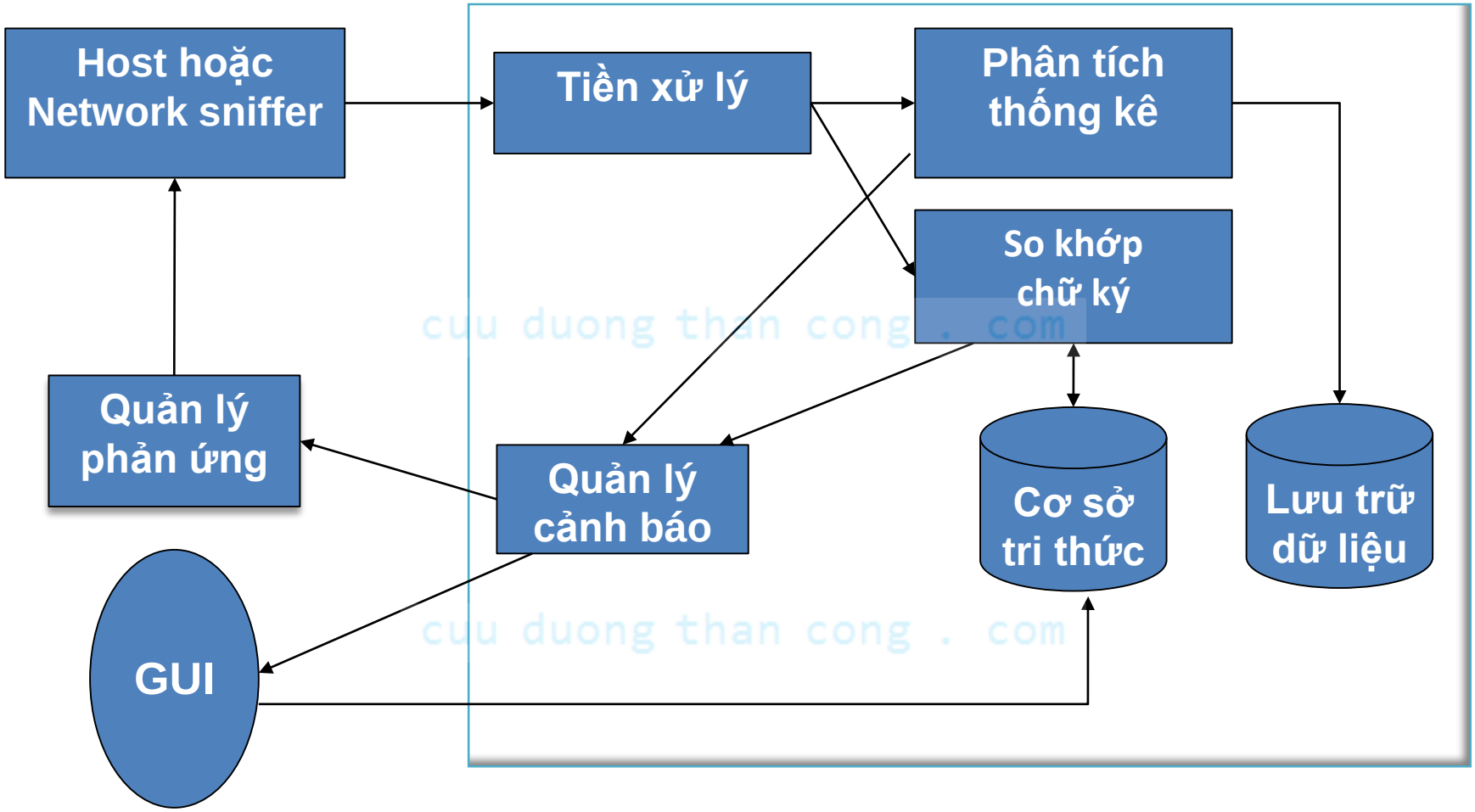
4.1. Giới thiệu IDS và IPS

- Phát hiện một hành vi vi phạm cấu hình và kích hoạt cảnh báo
- Nhiều IDS cho phép người quản trị cấu hình hệ thống để thông báo trực tiếp cho chúng về sự cố thông qua email hoặc máy nhắn tin
- Hệ thống cũng có thể được cấu hình để thông báo cho tổ chức cung cấp dịch vụ an toàn bên ngoài

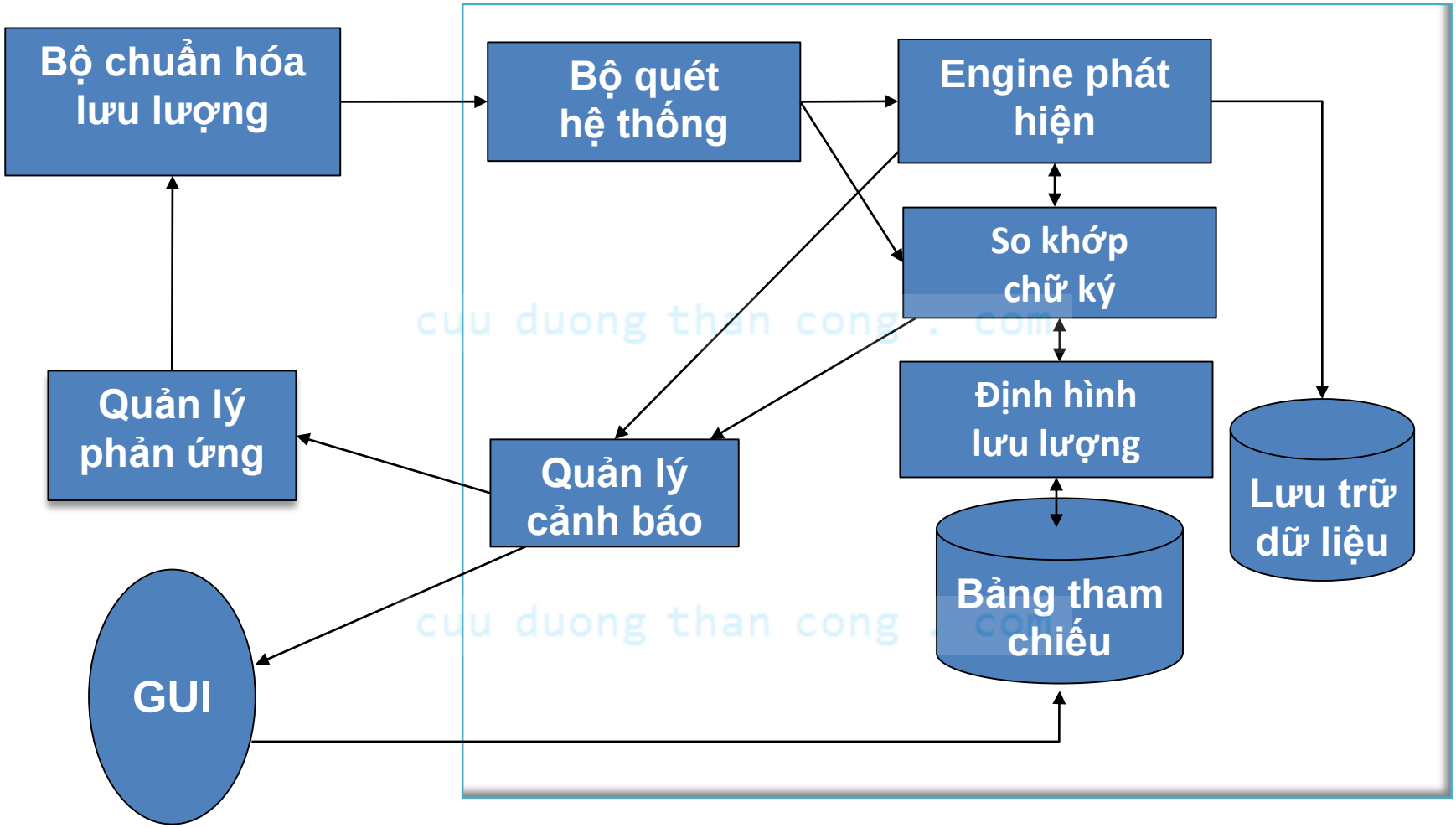
Phân biệt hệ thống IDS và IPS

- **IDS** là thiết bị phần cứng hoặc phần mềm mà giám sát mạng hoặc các hoạt động của hệ thống nhằm phát hiện ra sự phát tán của mã độc, hoặc sự vi phạm chính sách và đưa ra cảnh báo cho hệ thống và người quản trị
- **IPS** bao gồm các chức năng của IDS, ngoài ra có khả năng ngăn chặn sự phát tán mã độc và sự phi phạm chính sách

Kiến trúc của IDS



Kiến trúc của IPS



Các thuật ngữ

- Alert or alarm
- False attack stimulus
- False negative
- False positive
- Noise
- Site policy
- Site policy awareness
- True attack stimulus
- Confidence value
- Alarm filtering

Tại sao lại dùng IDPS?

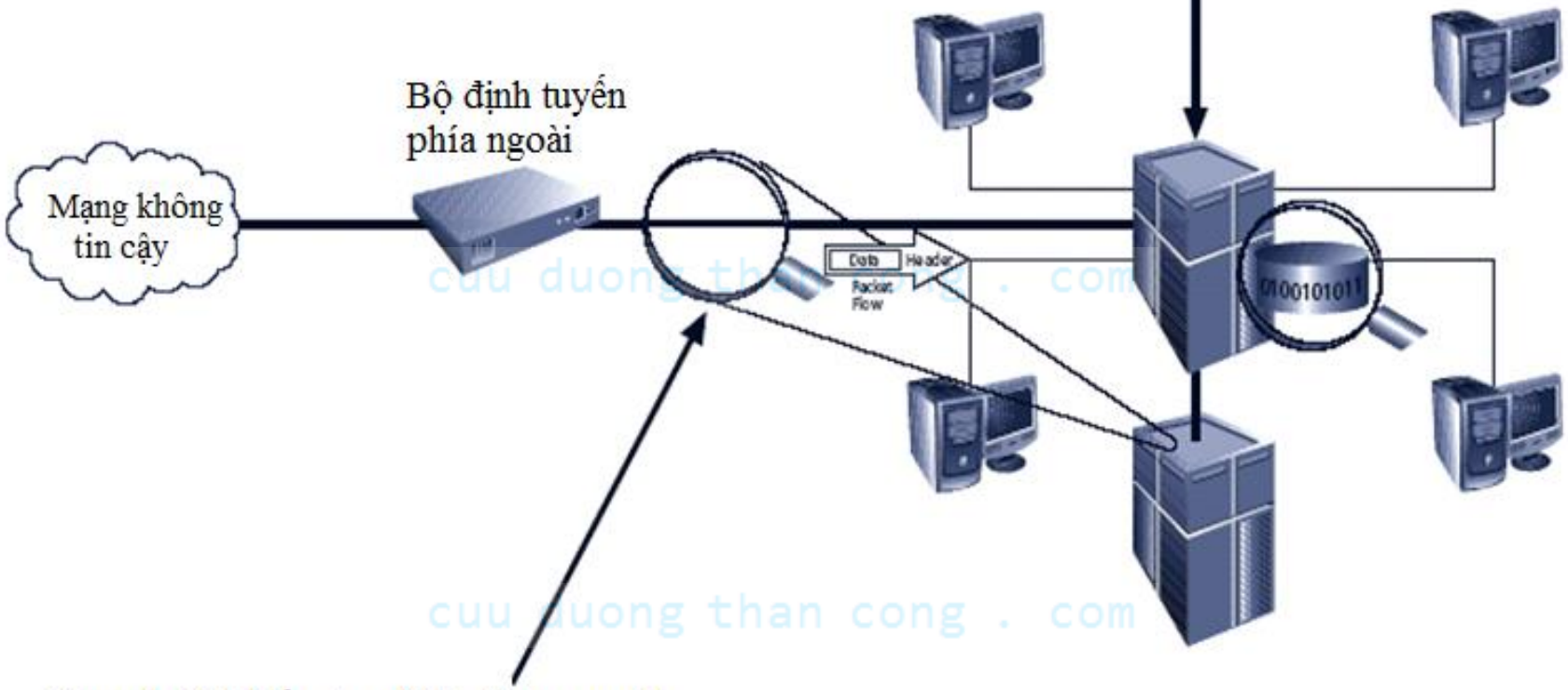
- Ngăn chặn hành vi có vấn đề bằng cách tăng các rủi ro nhận thức về phát hiện và trừng phạt
- Phát hiện các cuộc tấn công và vi phạm an ninh khác
- Phát hiện và đối phó với khởi đầu của các cuộc tấn công
- Lập tài liệu mối đe dọa hiện có cho tổ chức
- Kiểm soát chất lượng cho quản trị và thiết kế bảo mật, đặc biệt là các doanh nghiệp lớn và phức tạp
- Cung cấp thông tin hữu ích về sự xâm nhập diễn ra

Các loại hệ thống IDPS

- Các IDS hoạt động dựa trên mạng (network-based) hoặc dựa trên host (host-based)
- Tất cả các IDS dùng một trong ba phương pháp phát hiện:
  - Dựa trên dấu hiệu (Signature-based)
  - Dựa trên bất thường thống kê (Statistical anomaly-based)
  - Kiểm tra gói tin mang trang thái (Stateful packet inspection)

Các hệ thống IDS

Host IDS: kiểm tra dữ liệu trong các file lưu tại host và cảnh báo quản trị mạng về các thay đổi



Network IDS: kiểm tra gói tin trên mạng và cảnh báo quản trị mạng về các mẫu bất thường

Network-Based IDPS (NIDPS)

- Được đặt trên máy tính hoặc thiết bị kết nối với một phân đoạn mạng của tổ chức; tìm kiếm các dấu hiệu tấn công
- Khi kiểm tra các gói tin, NIDPS tìm kiếm các mẫu tấn công
- Được cài đặt tại một điểm cụ thể trên mạng nơi mà nó có thể theo dõi lưu lượng đi vào và đi ra khỏi phân đoạn mạng.

So khớp dấu hiệu NIDPS

- Để phát hiện một cuộc tấn công, NIDPS tìm kiếm mẫu tấn công
- Việc này được thực hiện bằng cách sử dụng cài đặt đặc biệt của chồng giao thức TCP/IP:
  - Trong quá trình chồng giao thức xác minh, NIDPS tìm kiếm các gói dữ liệu không hợp lệ
  - Trong xác minh giao thức ứng dụng, các giao thức tầng trên được kiểm tra về hành vi gói tin không mong muốn hoặc sử dụng không đúng cách.

Ưu điểm và nhược điểm của NIDPS

- Thiết kế mạng lưới và vị trí của NIDPS tốt cho phép tổ chức chỉ dùng một vài thiết bị có thể giám sát được mạng lớn
- NIDPS thường thụ động và có thể được triển khai với mạng có sẵn mà không làm gián đoạn đến hoạt động bình thường của mạng
- NIDPS thường không dễ bị tấn công trực tiếp và có thể không bị kẻ tấn công phát hiện

Ưu điểm và nhược điểm của NIDPS (tiếp)

- Có thể trở nên quá tải bởi khối lượng mạng và không nhận dạng được các tấn công
- Yêu cầu truy cập vào tất cả các lưu lượng được theo dõi
- Không thể phân tích các gói dữ liệu được mã hóa
- Không thể tin cậy xác định xem cuộc tấn công có thành công hay không
- Một số dạng tấn công không dễ dàng phân biệt bởi các NIDPS, đặc biệt là các dạng liên quan đến các gói tin bị phân mảnh

Host-Based IDPS

- Host-based IDP (HIDPS) được đặt tại một máy tính hoặc server cụ thể và chỉ giám sát hoạt động trên hệ thống đó
- Đánh giá và theo dõi tình trạng của các tập tin hệ thống quan trọng và phát hiện kẻ xâm nhập khi chúng tạo, chỉnh sửa, hoặc xóa các tập tin
- Hầu hết các công việc của HIDPS dựa trên nguyên tắc về cấu hình hoặc thay đổi về quản lý
- Lợi thế hơn NIDPS: thường được cài đặt để có thể truy cập thông tin mã hóa đi qua mạng

Ưu điểm và nhược điểm của HIDPS

- Đặt ra vấn đề quản lý nhiều hơn
- Dễ bị tổn thương trong cả hai trường hợp tấn công trực tiếp và tấn công chống lại hệ điều hành của host
- Không phát hiện được quét đa host, cũng không quét được các thiết bị mạng không thuộc host
- Dễ bị tấn công từ chối dịch vụ (DoS)
- Có thể sử dụng một lượng lớn không gian đĩa
- Có thể gây ra vượt quá hiệu năng trên các hệ thống host.

IDPS dựa trên dấu hiệu (Signature-Based IDPS)

- Kiểm tra lưu lượng dữ liệu trong khi tìm kiếm các mẫu so khớp với dấu hiệu đã biết
- Được sử dụng rộng rãi vì nhiều cuộc tấn công có dấu hiệu rõ ràng và khác biệt
- Vấn đề với cách tiếp cận này là khi chiến lược tấn công mới được xác định, cơ sở dữ liệu về dấu hiệu của IDPS phải liên tục được cập nhật

IDPS dựa trên bất thường thống kê (Statistical Anomaly-Based IDPS)

- Các IDPS dựa trên bất thường thống kê hoặc IDPS dựa trên hành vi lấy mẫu các hoạt động mạng để so sánh với lưu lượng đã được biết là bình thường
- Khi hoạt động đo được khác các mức ngưỡng, thì IDP sẽ kích hoạt một cảnh báo
- IDP có thể phát hiện kiểu tấn công mới
- Yêu cầu khả năng xử lý lớn hơn nhiều so với IDPS dựa trên dấu hiệu
- Có thể thường xuyên gây ra cảnh báo nhầm (false positive)

IDPS phân tích giao thức trạng thái (Stateful Protocol Analysis IDPS)

- SP 800-94: Phân tích giao thức trạng thái (SPA) tiến hành so sánh hồ sơ xác định trước của các định nghĩa của các hoạt động ôn hòa cho mỗi trạng thái giao thức đối với sự kiện quan sát để xác định độ lệch
- Lưu và sử dụng dữ liệu có liên quan được phát hiện trong một phiên để xác định sự xâm nhập liên quan đến nhiều yêu cầu/đáp ứng; cho phép IDPS phát hiện tốt các tấn công đa phiên (multisession) cụ thể (kiểm tra gói tin sâu).
- Nhược điểm: phức tạp khi phân tích; xử lý lớn; có thể không phát hiện được trừ khi giao thức vi phạm hành vi cơ bản; có thể gây ra vấn đề với giao thức mà nó kiểm tra

Giám sát tệp nhật ký (Log File Monitors)

- Giám sát tệp nhật ký (Log file monitor – LFM) tương tự như NIDPS
- Xem xét các log file được tạo ra bởi các server, các thiết bị mạng, và thậm chí IDPS khác cho các mẫu và dấu hiệu
- Các mẫu nhận biết tấn công dễ dàng được xác định khi toàn bộ mạng và hệ thống được xem xét toàn diện
- Yêu cầu phân bổ các nguồn lực đáng kể vì nó sẽ liên quan đến việc tập hợp, di chuyển, lưu trữ và phân tích một khối lượng lớn dữ liệu log

Hành vi đáp ứng IDPS

- Khi IDPS phát hiện một tình trạng mạng bất thường, nó sẽ có một số tùy chọn
- Các đáp ứng IDPS có thể được phân thành loại chủ động hoặc bị động
  - Đáp ứng chủ động: hành động được xác định ngay khi một loại cảnh báo nào đó được kích hoạt
  - Các tùy chọn đáp ứng bị động chỉ đơn giản là báo cáo

cuu duong than cong . com

Lựa chọn sản phẩm và cách tiếp cận IDPS

- Xem xét chính sách và kỹ thuật
  - Môi trường hệ thống của bạn là gì?
  - Mục đích và mục tiêu bảo mật của bạn là gì?
  - Chính sách bảo mật hiện tại của bạn là gì?
- Yêu cầu của tổ chức và các ràng buộc:
  - Yêu cầu được đánh từ bên ngoài tổ chức là gì?
  - Ràng buộc về tài nguyên của tổ chức là gì?

Lựa chọn sản phẩm và loại IDPS (tiếp)

- Tính năng và chất lượng của IDPS
  - Sản phẩm có đầy đủ khả năng mở rộng cho môi trường của bạn?
  - Làm thế nào có sản phẩm đã được thử nghiệm?
  - Mức người dùng về mục tiêu của sản phẩm là gì?
  - Sản phẩm có được thiết kế để phát triển theo sự phát triển của tổ chức?
  - Các quy định hỗ trợ cho sản phẩm là gì?

Điểm mạnh và hạn chế của IDPS

- IDPS thực hiện tốt các chức năng sau đây:
  - Giám sát và phân tích các sự kiện hệ thống và hành vi người dùng
  - Kiểm tra trạng thái an toàn về cấu hình hệ thống
  - Tạo ra trạng thái an ninh cơ sở cho hệ thống và theo dõi những thay đổi
  - Nhận ra được các mẫu sự kiện hệ thống để so khớp với các tấn công đã biết
  - Nhận ra được các mẫu hoạt động thay đổi từ hoạt động bình thường
  - Quản lý việc kiểm tra hệ điều hành và ghi lại (log) các kỹ thuật đã sử dụng và các dữ liệu đã được tạo ra

Điểm mạnh và hạn chế của IDPS (tiếp)

- IDPS thực hiện tốt các chức năng sau đây (tiếp):
  - Cảnh báo cho nhân viên thích hợp khi các phát hiện được có tấn công
  - Đo lường việc thực thi chính sách an toàn được mã hóa trong công cụ phân tích
  - Cung cấp các chính sách an toàn thông tin mặc định
  - Cho phép các chuyên gia không phải về an toàn có thể thực hiện các chức năng giám sát an toàn quan trọng

Điểm mạnh và hạn chế của IDPS (tiếp)

- IDPS không thể thực hiện các chức năng sau:
  - Bồi thường cho các kỹ thuật bảo mật thiếu/yếu kém trong cơ sở hạ tầng bảo vệ
  - Ngay lập tức phát hiện, báo cáo, ứng phó với tấn công khi có hiện tượng tải mạng nặng
  - Phát hiện các cuộc tấn công mới hoặc các biến thể của các cuộc tấn công hiện tại
  - …

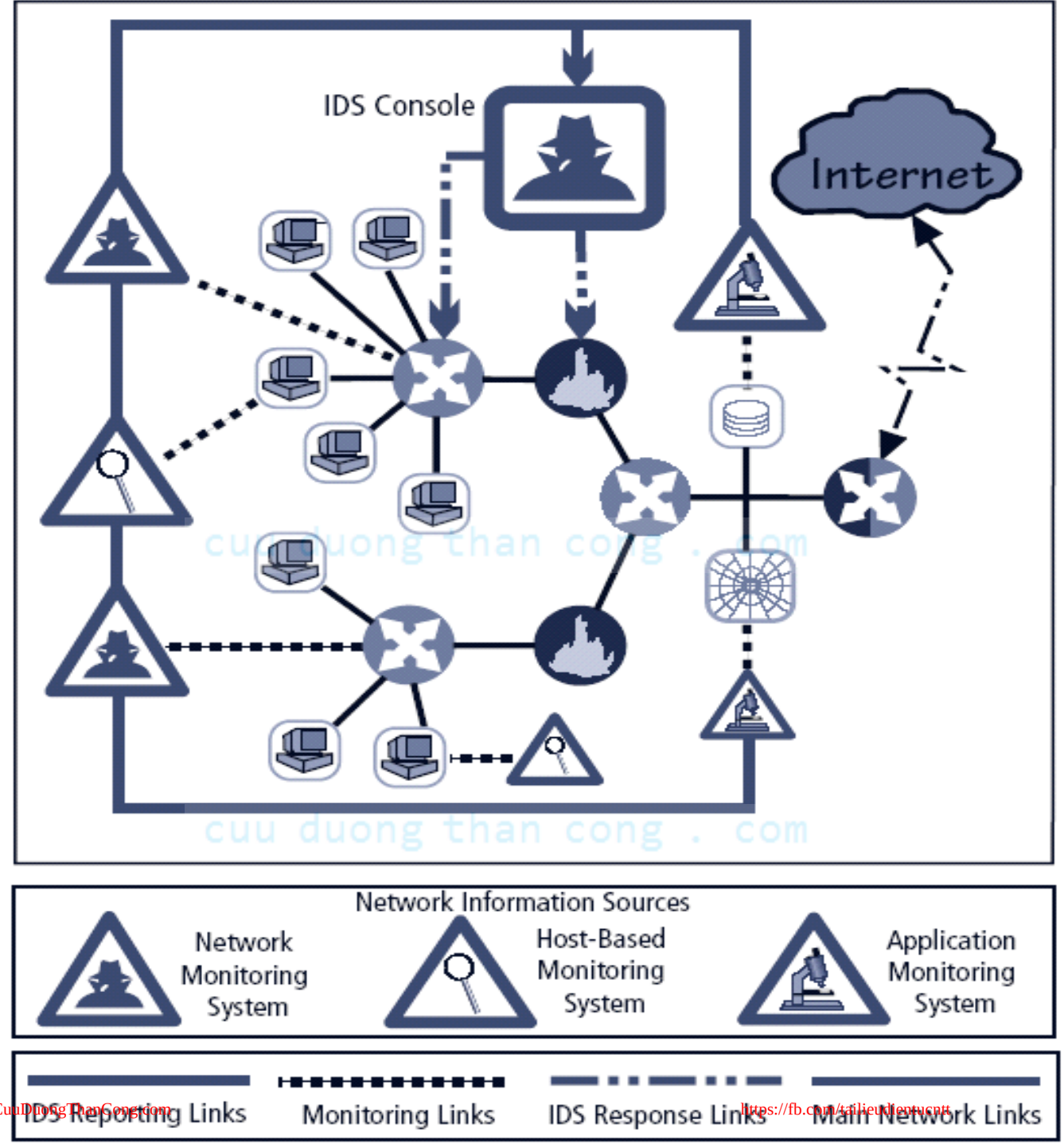
Điểm mạnh và hạn chế của IDPS (tiếp)

- IDPS không thể thực hiện các chức năng sau:
  - …
  - Phản ứng hiệu quả với các cuộc tấn công từ những kẻ tấn công tinh vi
  - Điều tra các cuộc tấn công không có sự can thiệp của con người
  - Chống lại các cuộc tấn công có ý định cản trở hoặc phá vỡ chúng
  - Bồi thường cho các vấn đề liên quan đến độ trung thực của các nguồn dữ liệu
  - Đối phó hiệu quả với các mạng chuyển mạch

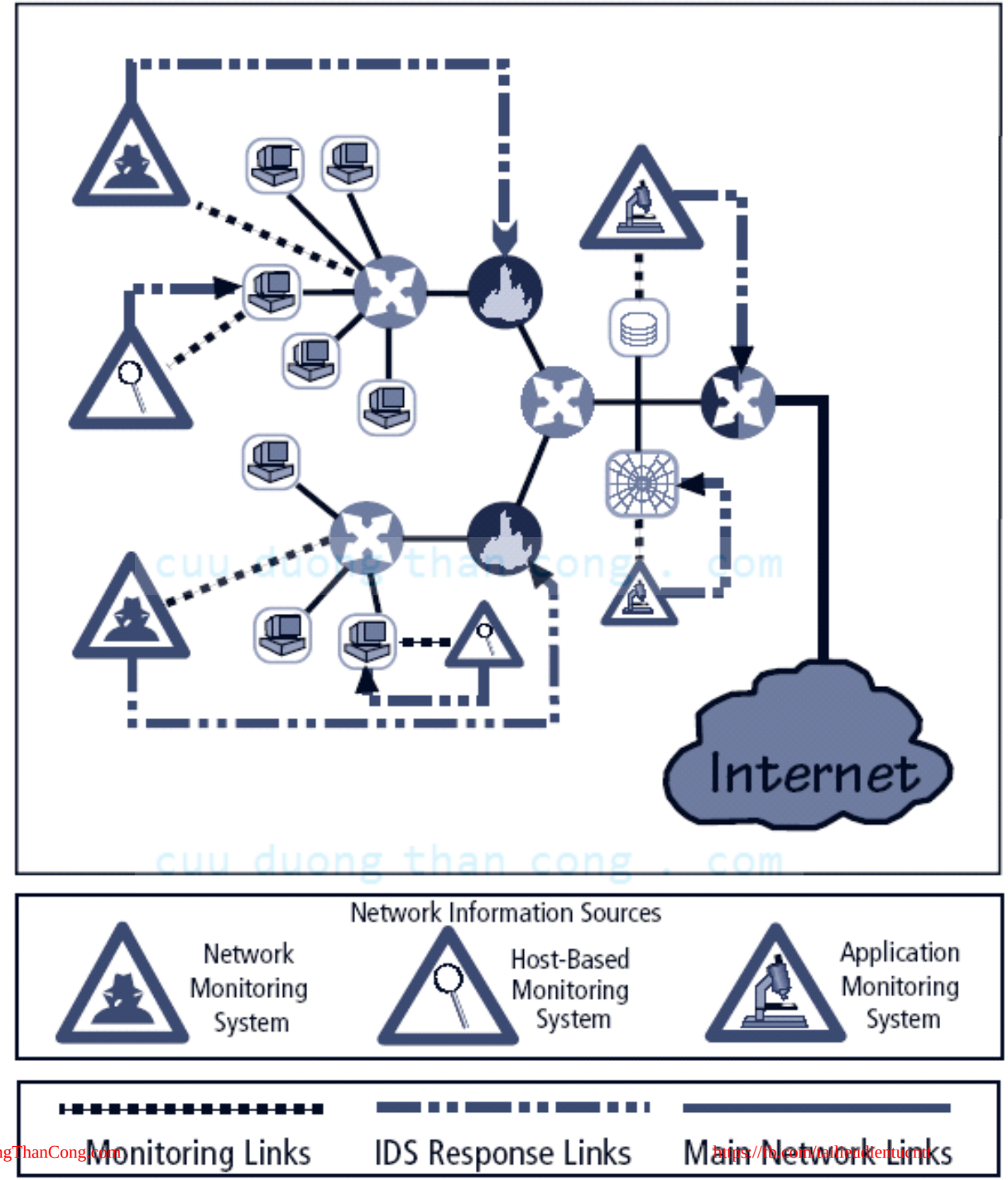
Các chiến lược điều khiển của IDPS

- Một IDPS có thể được cài đặt thông qua một trong ba chiến lược điều khiển cơ bản
  - Tập trung: tất cả các chức năng điều khiển của IDPS được cài đặt và quản lý tại một vị trí trung tâm
  - Phân phối đầy đủ: tất cả các chức năng điều khiển được áp dụng tại vị trí vật lý của mỗi thành phần IDPS
  - Phân phối từng phần: kết hợp cả hai; trong khi các agent cá nhân vẫn có thể phân tích và phản ứng với các mối đe dọa cục bộ, thì chúng có thể báo cáo đến các cơ sở trung tâm phân cấp để cho phép tổ chức phát hiện ra các cuộc tấn công trên diện rộng

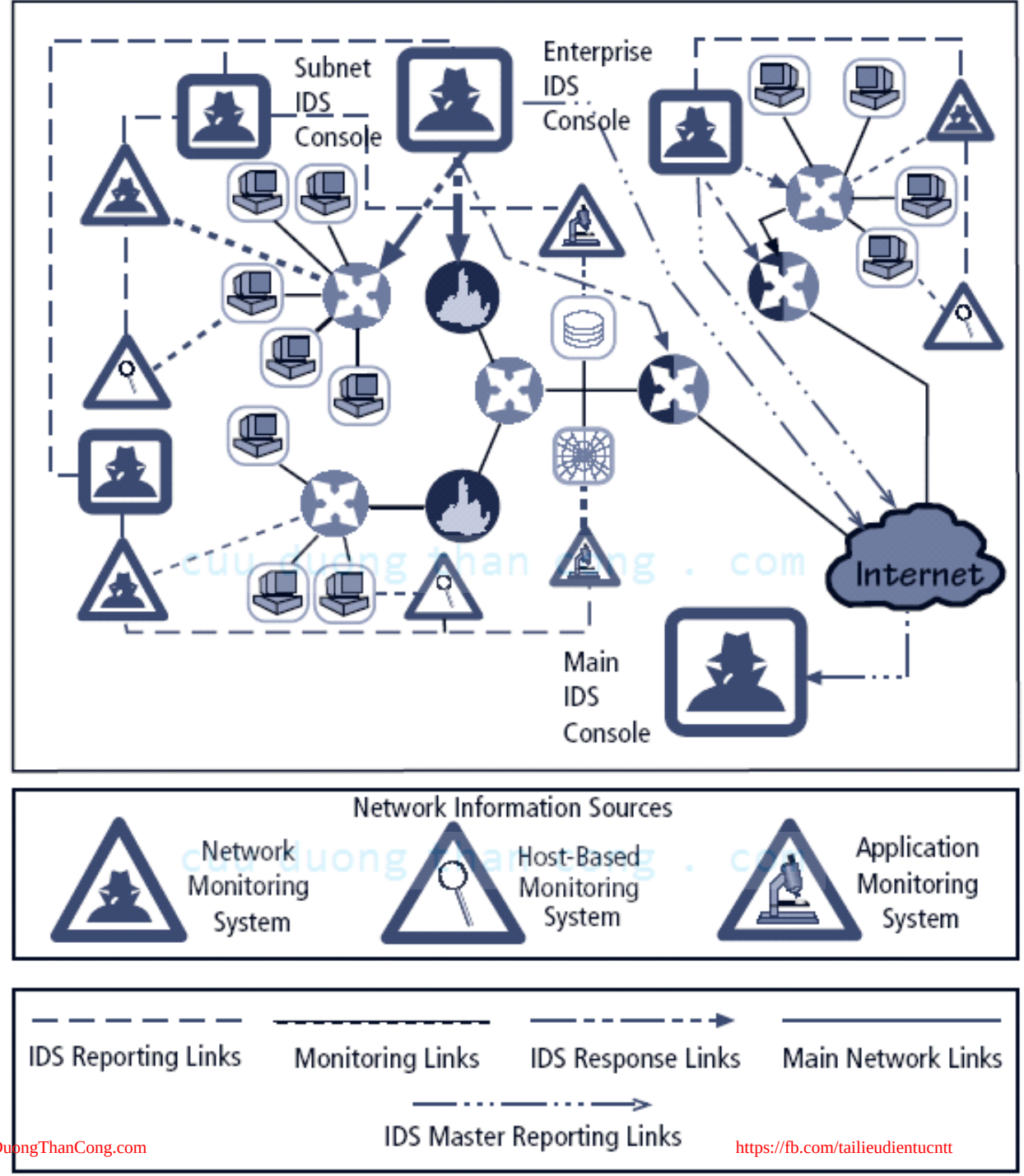
Kiểm soát IDS tập trung



Kiểm soát IDS hoàn toàn phân tán



Kiểm soát IDS phân tán một phần



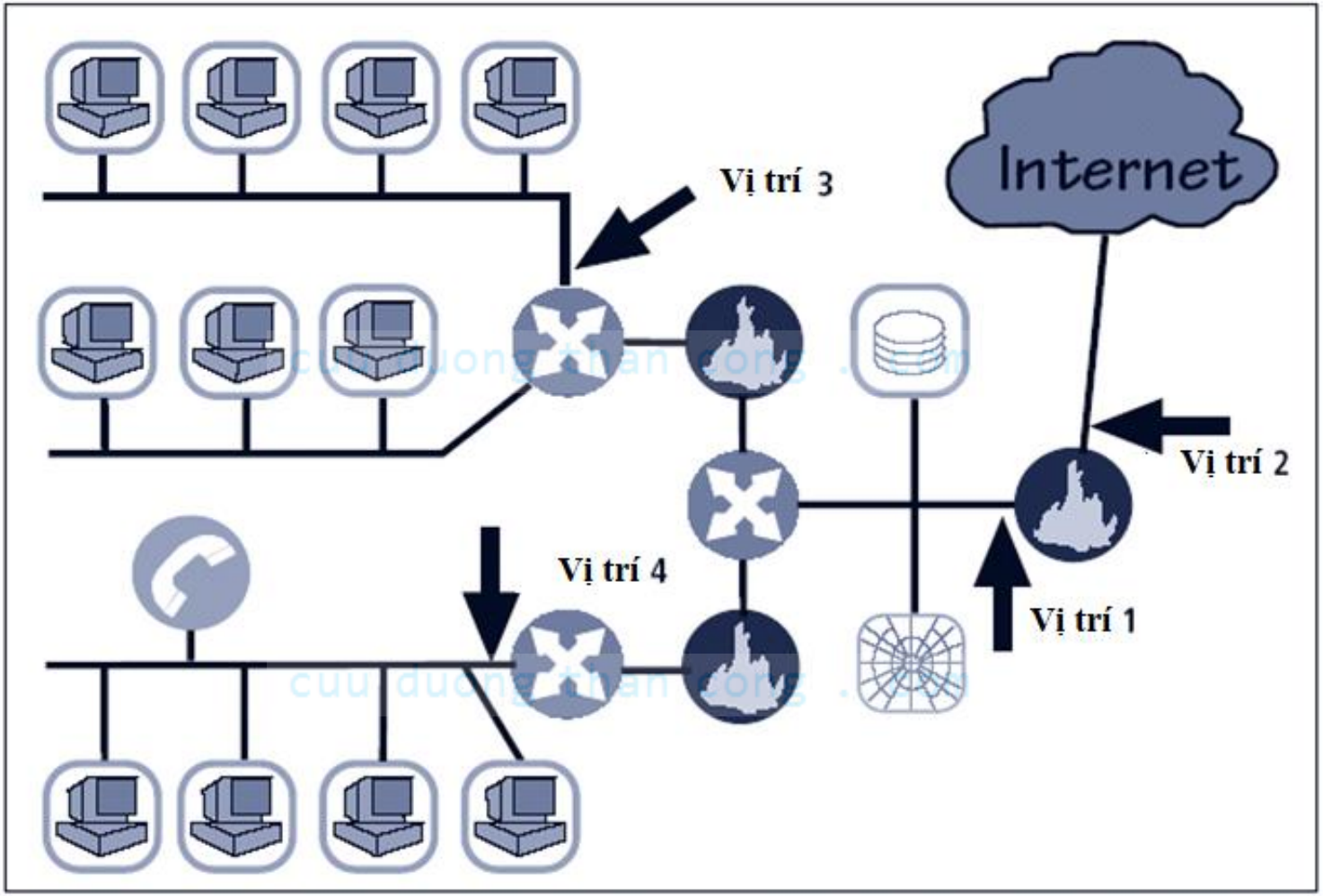
Triển khai IDPS

- Giống như các chiến lược kiểm soát quyết định liên quan, quyết định vị trí đặt các phần tử của hệ thống phát hiện xâm nhập là một nghệ thuật
- Khi xây dựng kế hoạch phải chọn chiến lược triển khai dựa trên việc phân tích kỹ lưỡng những yêu cầu bảo mật thông tin của tổ chức, đồng thời gây tác động tối thiểu tới tổ chức
- NIDPS và HIDPS có thể được sử dụng song song để bao phủ cả các hệ thống riêng được kết nối tới mạng của tổ chức và cả hệ thống mạng

Triển khai Network-Based IDPSs

- NIST khuyến nghị 4 vị trí cho các cảm biến NIDPS
  - Vị trí 1: Đằng sau mỗi tường lửa ngoài, trong DMZ mạng
  - Vị trí 2: Bên ngoài một tường lửa ngoài
  - Vị trí 3: Trên mạng xương sống chính
  - Vị trí 4: Trên các mạng con quan trọng

Các vị trí đặt sensor của IDS mạng



Triển khai Host-Based IDPS

- Cài đặt đúng các HIDPS là một công việc vất vả và tốn nhiều thời gian
- Trước tiên, bắt đầu với việc cài đặt các hệ thống quan trọng nhất
- Tiếp tục cài đặt cho đến khi tất cả các hệ thống được cài đặt hoàn toàn, hoặc tổ chức đạt được mức kế hoạch đủ bảo đảm hệ thống sẵn sàng

Đo lường hiệu quả của IDPS

- IDPS được đánh giá bằng cách sử dụng bốn số liệu chi phối: ngưỡng, danh sách đen và danh sách cho phép, các thiết lập cảnh báo, và xem và sửa mã
- Đánh giá IDPS: vd mức có thể đọc 100 Mb/s, hay IDS đã có thể phát hiện 97% các cuộc tấn công trực tiếp
- Phát triển tập này có thể khá tẻ nhạt, nhưng hầu hết các nhà cung cấp IDPS đều cung cấp kỹ thuật kiểm tra xác minh rằng hệ thống được thực hiện như mong đợi

Đo lường hiệu quả của IDPS (tiếp)

- Một vài trong số các tiến trình thử nghiệm này sẽ cho phép các quản trị viên:
  - Ghi và truyền lại các gói tin từ một tiến trình quét virus/sâu thật sự
  - Ghi và truyền lại các gói tin từ một tiến trình quét virus/sâu thật sự với phiên kết nối TCP/IP không đầy đủ (thiếu các gói SYN)
  - Quét virus/sâu để có được một hệ thống không có điểm yếu

5. Honeypot, Honeynet và hệ thống Padded Cell

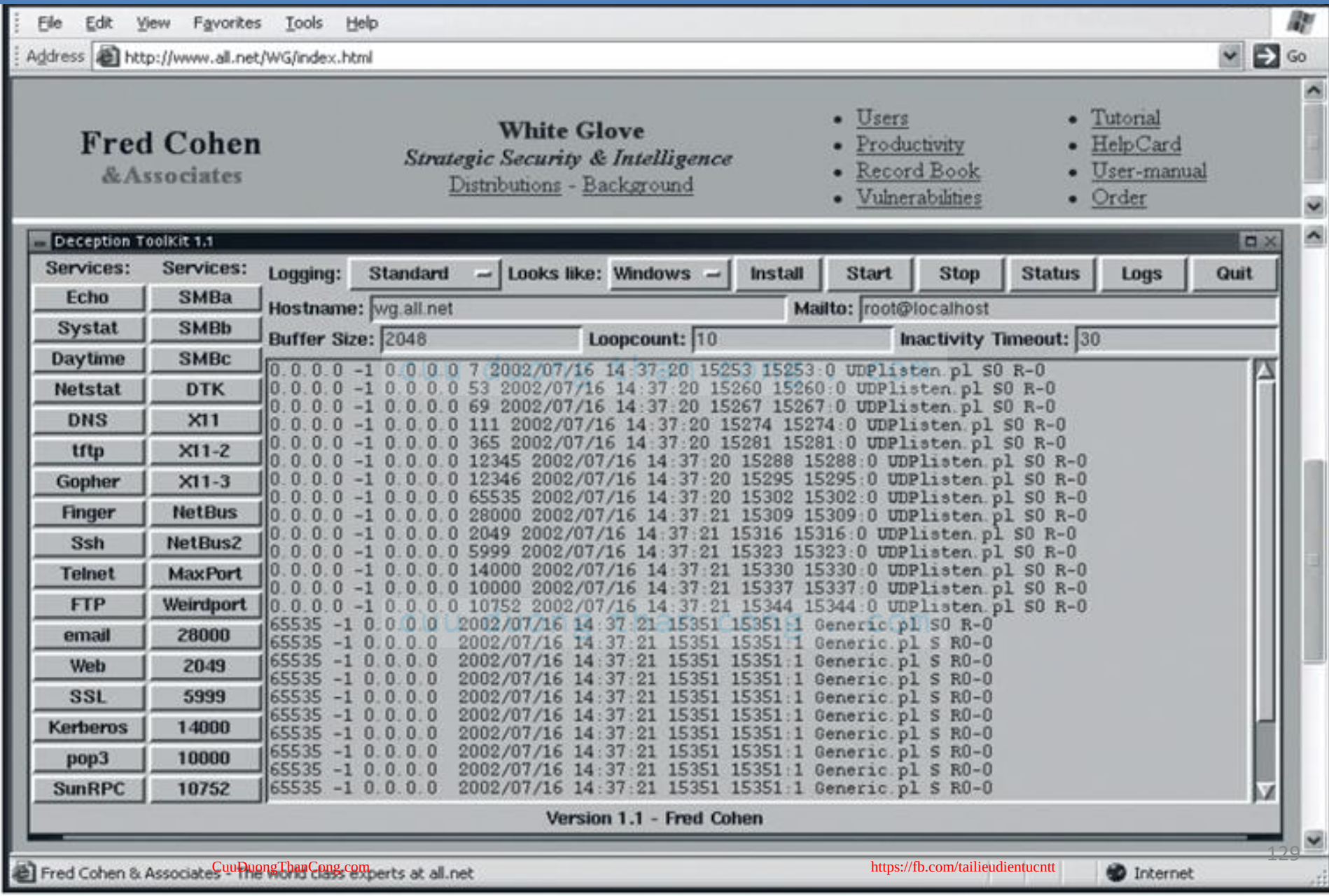
5. Honey Pot, Honey Net và hệ thống Padded Cell

1. Honey pot, Honey net và hệ thống Padded cell
2. Các hệ thống bẫy và tìm vết
3. Ngăn chặn xâm nhập tích cực

5.1. Honey Pot, Honey Net và hệ thống Padded Cell

- Honey pot: hệ thống mồi được thiết kế để thu hút những kẻ tấn công tiềm năng tránh xa các hệ thống quan trọng và khuyến khích các cuộc tấn công chống lại chính mình
- Honey net: tập các honey pot, kết nối một số hệ thống honey pot trên một subnet
- Honey pot được thiết kế để:
  - Chuyển hướng kẻ tấn công truy cập vào hệ thống quan trọng
  - Thu thập thông tin về hoạt động của kẻ tấn công
  - Khuyến khích kẻ tấn công ở lại trên hệ thống đủ dài để các quản trị viên ghi lại sự kiện, và có thể đáp trả

Bộ công cụ mồi



Honey Pot, Honey Net và hệ thống Padded Cell (tiếp)

- Tế bào đệm (Padded Cell): honey pot đã được bảo vệ vì vậy nó không thể dễ dàng bị xâm nhập
- Ngoài việc thu hút những kẻ tấn công với các dữ liệu hấp dẫn, một tế bào đệm còn hoạt động song song với một IDS truyền thống
- Khi IDS phát hiện được kẻ tấn công, nó sẽ chuyển chúng vào một môi trường mô phỏng đặc biệt, nơi có thể không gây hại

Honey Pot, Honey Net và hệ thống Padded Cell (tiếp)

- Ưu điểm
  - Kẻ tấn công có thể được chuyển hướng đến mục tiêu mà chúng không thể phá hủy
  - Các quản trị viên có thời gian để quyết định xem đối phó với kẻ tấn công như thế nào
  - Những hành động của kẻ tấn công có thể được theo dõi một cách dễ dàng và rộng rãi hơn, và các bản ghi có thể được sử dụng để tinh chỉnh các mẫu nguy cơ và cải thiện các biện pháp bảo vệ hệ thống
  - Honey pot có thể hiệu quả trong việc bắt những người từ bên trong đang rình mò xung quanh mạng

Honey Pot, Honey Net và hệ thống Padded Cell (tiếp)

- Nhược điểm:
  - Ý nghĩa pháp lý của việc sử dụng các thiết bị này không được xác định rõ
  - Honey pot và các tế bào đệm vẫn chưa được chứng minh là có công nghệ bảo mật hữu ích chung
  - Kẻ tấn công chuyên nghiệp, khi đã bị chuyển hướng vào trong một hệ thống mồi, có thể trở nên tức giận và sẽ khởi động một cuộc tấn công thù địch hơn chống lại các hệ thống hệ thống của một tổ chức
  - Quản trị viên và các nhà quản lý bảo mật sẽ cần đạt được mức độ chuyên môn cao để sử dụng các hệ thống này.

5.2. Các hệ thống bẫy và tìm vết

- Sử dụng kết hợp các kỹ thuật phát hiện xâm nhập và tìm dấu vết nó quay về nguồn
- Bẫy (trap) thường bao gồm honey pot hoặc tế bào đệm và báo động
- Hạn chế pháp lý với bẫy và tìm vết
  - Dụ dỗ: quá trình thu hút sự chú ý đến hệ thống bằng cách đặt bit thông tin trêu ngươi tại các địa điểm quan trọng
  - Bẫy : hành động thu hút một cá nhân thực hiện hành vị phạm pháp
  - Dụ dỗ là hợp pháp và có đạo đức, trong khi đó bẫy thì không.

5.3. Phòng ngừa xâm nhập chủ động

- Một số tổ chức cài đặt các biện pháp đối phó tích cực để ngăn chặn các cuộc tấn công
- Một công cụ (LaBrea) chiếm không gian địa chỉ IP không sử dụng để giả vờ là một máy tính và cho phép kẻ tấn công hoàn thành một yêu cầu kết nối, nhưng sau đó giữ kết nối mở.