Chương 1

Những vấn đề cơ bản về an toàn thông tin

1. Thông tin

- Định nghĩa: Thông tin là những tính chất xác định của vật chất mà con người (hoặc hệ thống kỹ thuật) nhận được từ thế giới vật chất bên ngoài hoặc từ những quá trình xảy ra trong bản thân nó.
- Thông tin tồn tại một cách khách quan, không phụ thuộc vào hệ thụ cảm.

2. Khái niệm hệ thống và tài nguyên thông tin

- Khái niệm hệ thống: Hệ thống là một tập hợp các máy tính gồm thành phần phần cứng, phần mềm và dữ liệu làm việc được tích luỹ qua thời gian.
- Tài nguyên thông tin:
  - ✓ Phần cứng
  - ✓ Phần mềm
  - ✓ Dữ liệu
  - ✓ Môi trường truyền thông giữa các máy tính
  - ✓ Môi trường làm việc
  - ✓ Con người

3. Các mối đe doạ đối với một hệ thống TT và các biện pháp ngăn chặn

- Phá hoại: Phá hỏng thiết bị phần cứng hoặc phần mềm trên hệ thống.
- Sửa đổi: Tài sản của hệ thống bị sửa đổi trái phép.
- Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền. Các hành vi : Đánh cắp mật khẩu , ngăn chặn,mạo danh…

Có ba loại đối tượng chính khai thác

- *Inside* :các đối tượng từ bên trong hệ thống , đây là những người có quyền truy cập hợp pháp đối với hệ thống
- *Outside*: hacker , cracker….
- *Phần mềm* : Virut, spyware,mainware và các lỗ hổng phần mềm : SQL injnection …

4. Các biện pháp ngăn chặn:

Thường có 3 biện pháp ngăn chặn:

- Thông qua phần mềm: Sử dụng các thuật toán mật mã học tại các cơ chế an toàn bảo mật của hệ thống mức hệ điều hành.
- Thông qua phần cứng: Sử dụng các hệ MM đã được cứng hóa .
- Thông qua các chính sách AT& BM Thông tin do tổ chức ban hành nhằm đảm bảo an toàn bảo mật của hệ thống.

Tại sao ?

- Thiếu hiểu biết và kinh nghiệm để bảo vệ dữ liệu
- An toàn là một lãnh vực phát triển cao trong công nghệ TT, nhu cầu về nguồn nhân lực trong lĩnh vực này đang tăng lên rất nhanh
- Liên quan đến nghề nghiệp của bạn
- Sự phát triển công nghệ thông tin

5.An toàn thông tin là gì

- An toàn thông tin bao hàm một lĩnh vực rộng lớn các hoạt động trong một tổ chức. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin, kiến thức, dữ liệu.
- Mục đích là đảm bảo một môi trường thông tin tin cậy , an toàn và trong sạch cho mọi thành viên và tổ chức trong xã hội

6. Nguyên tắc , mục tiêu và chung của an toàn bảo mật thông tin

Hai nguyên tắc của an toàn bảo mật thông tin:

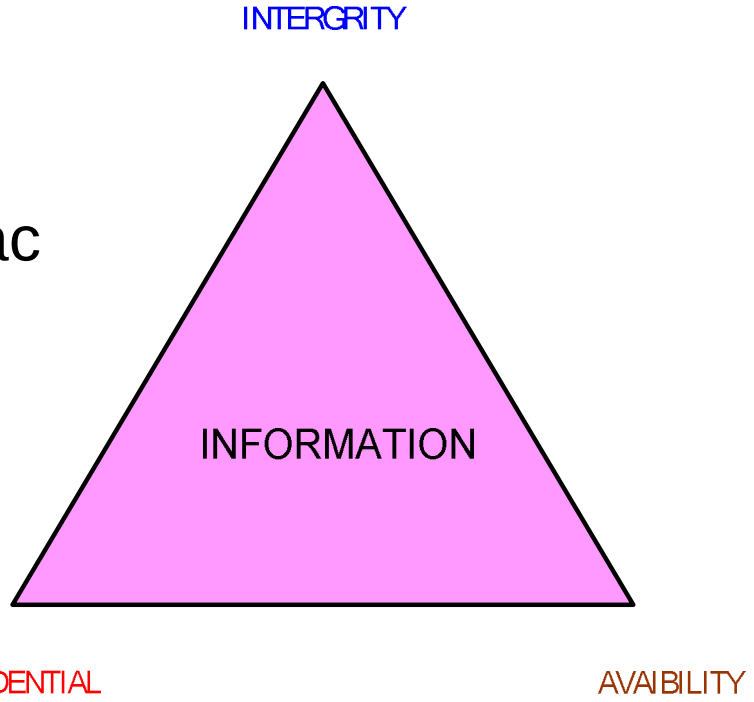
- Việc thẩm định về bảo mật phải đủ khó và cần tính tới tất cả các tình huống , khả năng tấn công có thể được thực hiện.
- Tài sản phải được bảo vệ cho tới khi hết gía trị sử dụng hoặc hết ý nghĩa bí mật.

Tính chất của hệ thống thông tin

- Nguồn thông tin là những tài sản rất có giá trị của một tổ chức.Thậm chí mang tính sống còn.
- Sự yếu kém và dễ bị tấn công của các hệ thống thông tin.
- Nhiều vấn đề về an ninh cần phải quan tâm, từ đó có một lý do chính đáng để thay đổi phương thức bảo mật thông tin, mạng, máy tính của bạn

Mục tiêu của An toàn Thông tin

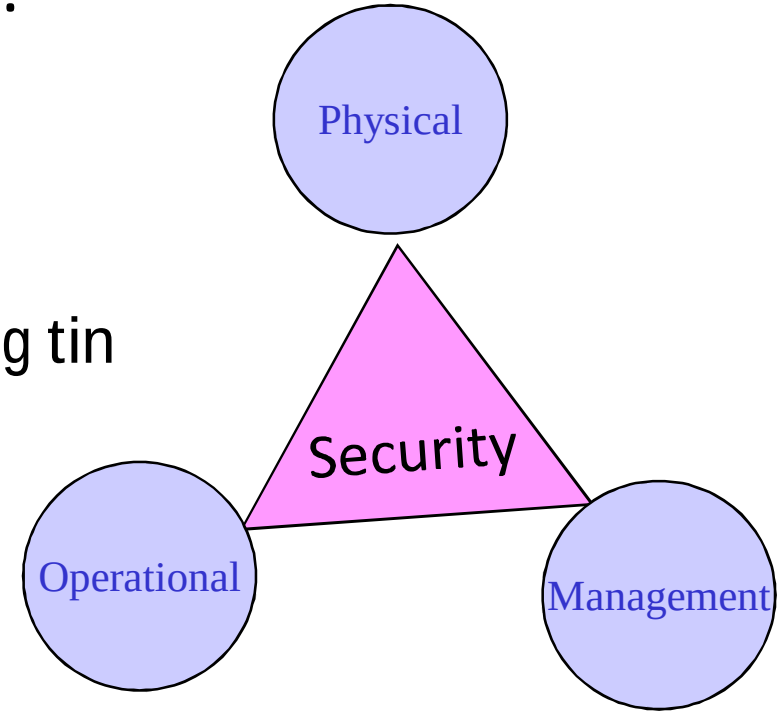
- Bí mật - CONFIDENCIAL
- Toàn vẹn – INTEGRITY,Tính xác thực - AUTHORITY
- Sẵn sàng - AVAIBILITY



THÔNG TIN – ĐỐI TƯỢNG CỦA CÁC CUỘC TẤN CÔNG

7. Các thành phần chính của ATTT

- An toàn mức vật lý.
- An toàn mức tác nghiệp.
- Quản lý và chính sách.



Hình 1 - Tam giác an toàn thông tin

7.1.An toàn vật lý

- An toàn ở mức vật lý là sự bảo vệ tài sản và thông tin của bạn khỏi sự truy cập vật lý không hợp lệ .
- Đảm bảo an toàn mức vật lý tương đối dễ thực hiện .
- Biện pháp bảo vệ đầu tiên là làm sao cho vị trí của tổ chức càng ít trở thành mục tiêu tấn công càng tốt .
- Biện pháp bảo vệ thứ hai phát hiện và ngăn chặn các kẻ đột nhập hay kẻ trộm : camera , t/b chống trộm.
- Biện pháp bảo vệ thứ ba là khôi phục những dữ liệu hay hệ thống cực kỳ quan trọng bị trộm hay mất mát.

Thao tác an toàn

- Thao tác an toàn liên quan những gì mà một tổ chức cần thực hiện để đảm bảo một chính sách an toàn . Thao tác này bao gồm cả hệ thống máy tính, mạng, hệ thống giao tiếp và quản lý thông tin. Do đó thao tác an toàn bao hàm một lãnh vự rộng lớn và vì bạn là một chuyên gia an toàn nên bạn phải quan tâm trực tiếp đến các lãnh vực này.

7.2.Quy trình thao tác an tòan

- Vấn đề đặt ra cho thao tác an toàn gồm :
- Kiểm soát truy cập,
- Chứng thực,
- An toàn topo mạng sau khi việc thiết lập mạng
- Các thao tác an toàn trên đây không liên quan đến việc bảo vệ ở mức vật lý và mức thiết kế

Quy trình thao tác an toàn

- Sự kết hợp của tất cả các quá trình, các chức năng và các chính sách bao gồm cả yếu tố con người và yếu tố kỹ thuật.
- Yếu tố con người tập trung vào các chính sách được thực thi trong tổ chức.
- Yếu tố kỹ thuật bao gồm các công cụ mà ta cài đặt vào hệ thống.
- Quá trình an toàn này được chia thành nhiều phần và được mô tả dưới đây:

Quy trình an toàn (cont.)

a. Phần mềm chống virus

- Virus máy tính là và vấn đề phiền toái nhất
- Các phương thức chống virus mới ra đời cũng nhanh tương tự như sự xuất hiện của chúng
- File chống virus được cập nhận mỗi hai tuần một lần hay lâu hơn. Nếu các file này cập nhật thường xuyên thì hệ thống có thể là tương đối an toàn.
- Phát hiện và diệt virut trực tuyến

Quy trình an toàn (cont.)

b. Kiểm soát truy cập

- ✓ Kiểm soát truy cập bắt buộc (MAC – Mandatory Access Control):Cách truy cập tĩnh, sử dụng một tập các quyền truy cập được định nghĩa trước đối với các file trong hệ thống.
- ✓ Kiểm soát truy cập tự do (DAC – Discretionary Access Control) : Do chủ tài nguyên cấp quyền thiết lập một danh sách kiểm soát truy cập (ACL – Access Control List) .
- ✓ Kiểm soát truy cập theo vai trò (chức vụ) (RBAC – Role Based Access Control) : Truy cập với quyền hạn được xác định trước trong hệ thống, quyền hạn này căn cứ trên chức vụ của người dùng trong tổ chức

c. Chứng thực (authentication)

- ✓ Chứng minh " Tôi chính là tôi chứ không phải ai khác "
- ✓ Là một phần quan trọng trong ĐỊNH DANH và CHỨNG THỰC (Identification & Authentication – I &A).

Ba yếu tố của chứng thực :

- Cái bạn biết (Something you know)– Mật mã hay số PIN
- Cái bạn có (Something you have) – Một card thông minh hay một thiết bị chứng thực
- Cái bạn sở hữu (Something you are) – dấu vân tay hay võng mạc mắt của bạn

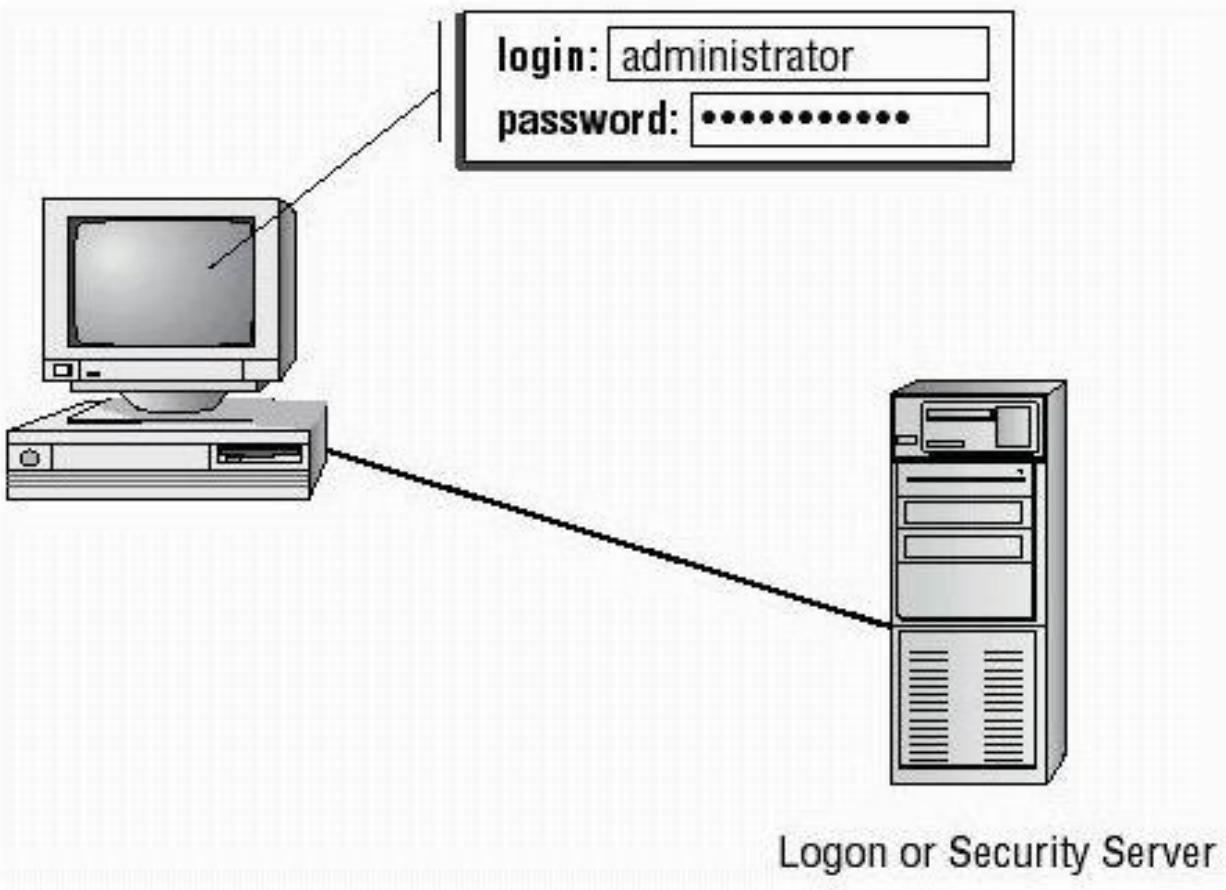
Những phương thức chứng thực thông dụng

- *Dùng username/Password :*

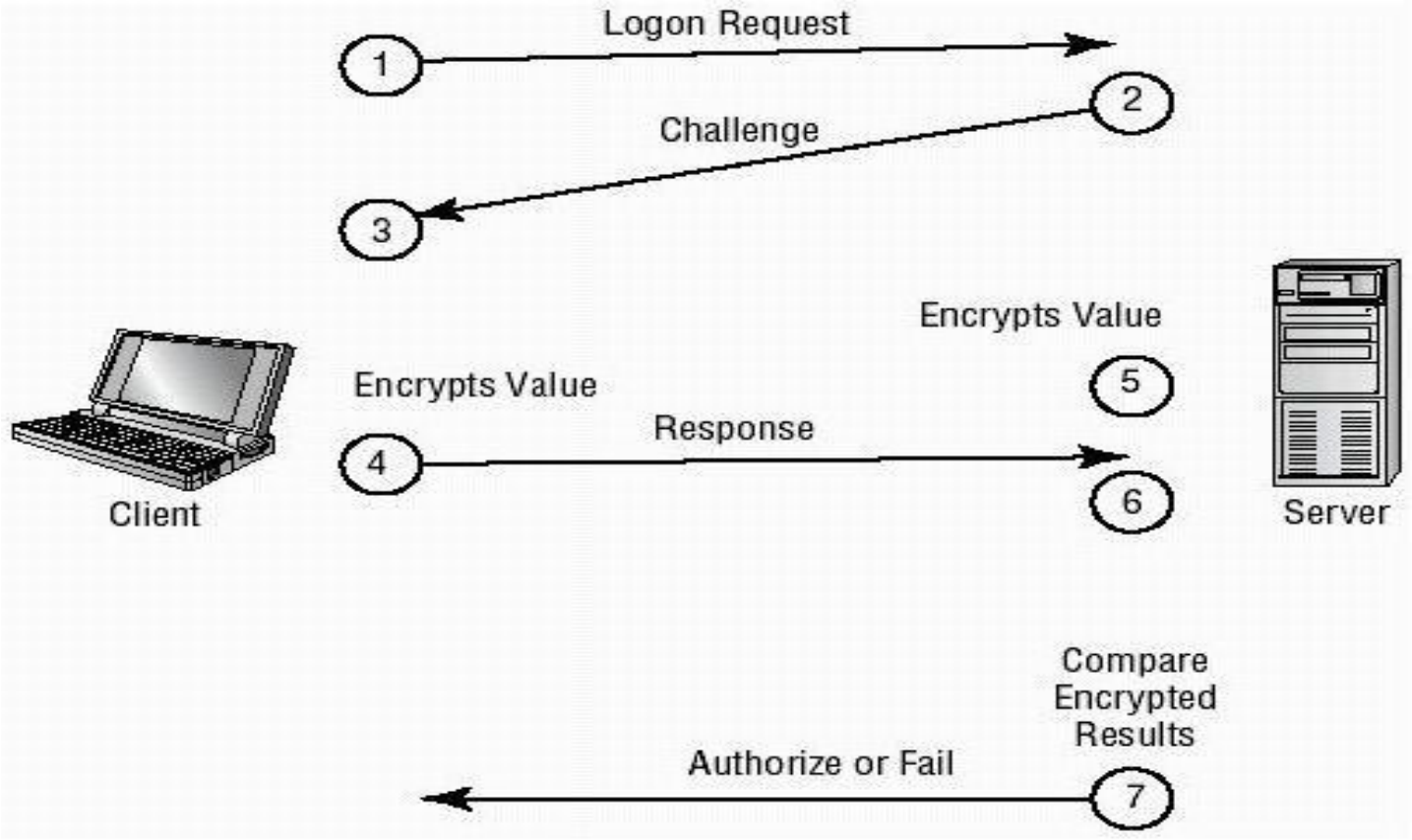
  ✓ Một tên truy cập và một mật khẩu là định danh duy nhất để đăng nhập . Bạn là chính bạn chứ không phải là người giả mạo

  ✓Server sẽ so sánh những thông tin này với những thông tin lưu trữ trong máy bằng các phương pháp xử lý bảo mật và sau đó quyết định chấp nhận hay từ chối sự đăng nhập

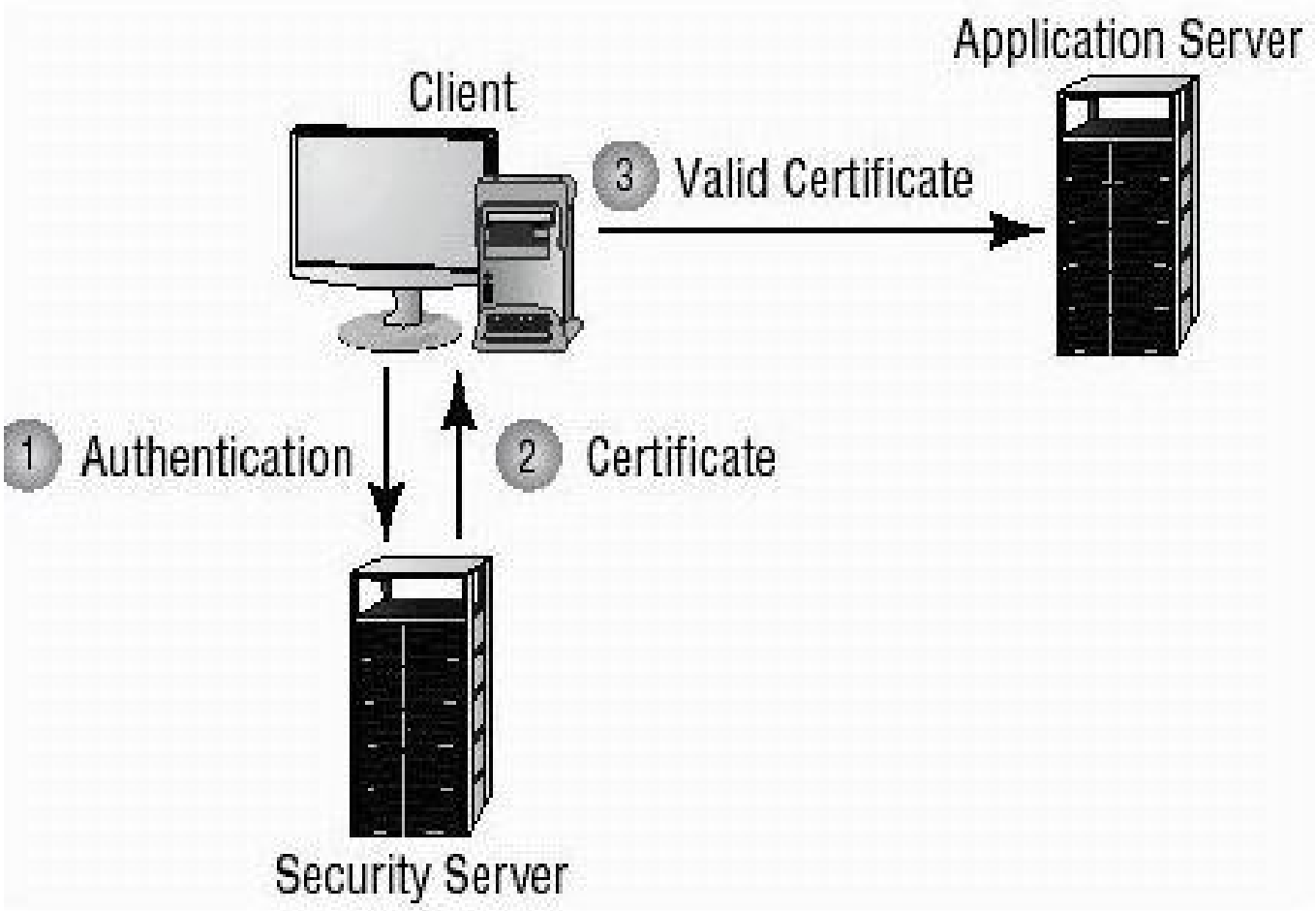
Sử dụng Username/Password



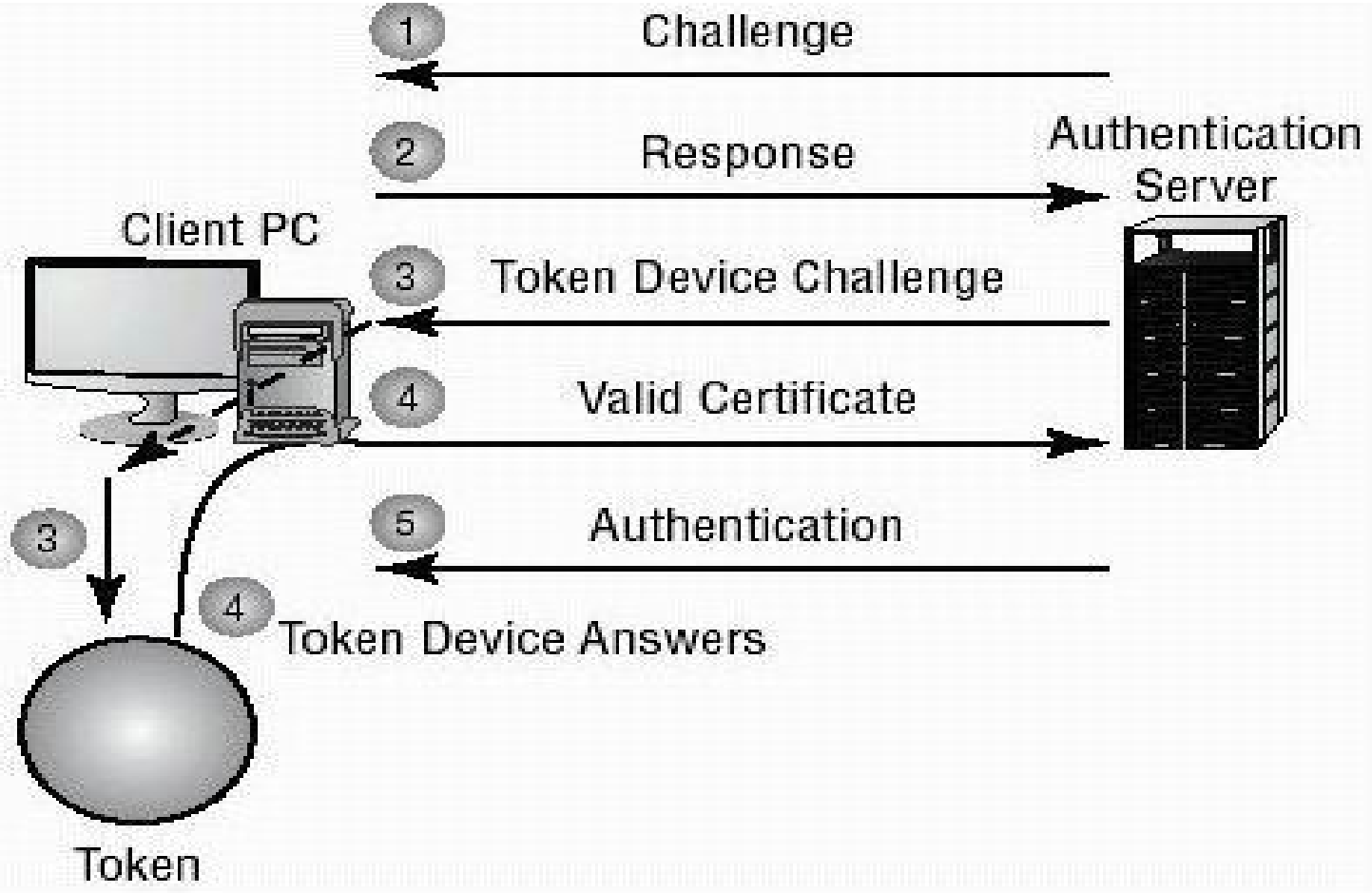
Giao thức chứng thực CHAP – (Challenge HandShake Authentication Protocol) :



Chứng chỉ : Certificate Authority (CA)

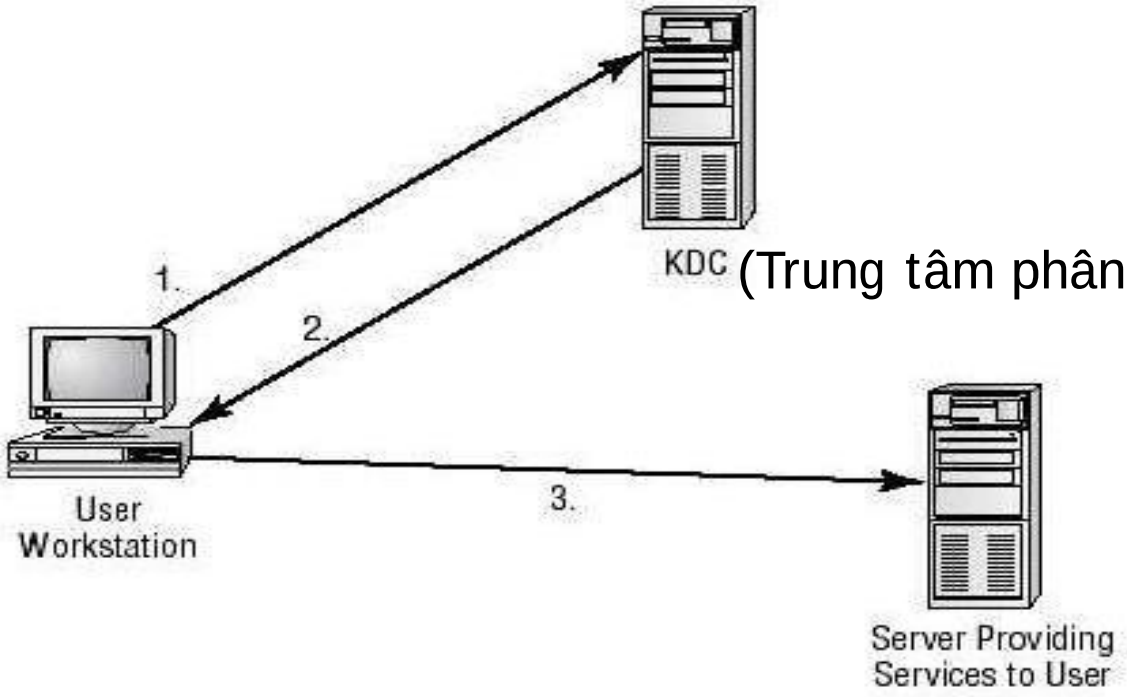


Bảo mật bằng token:



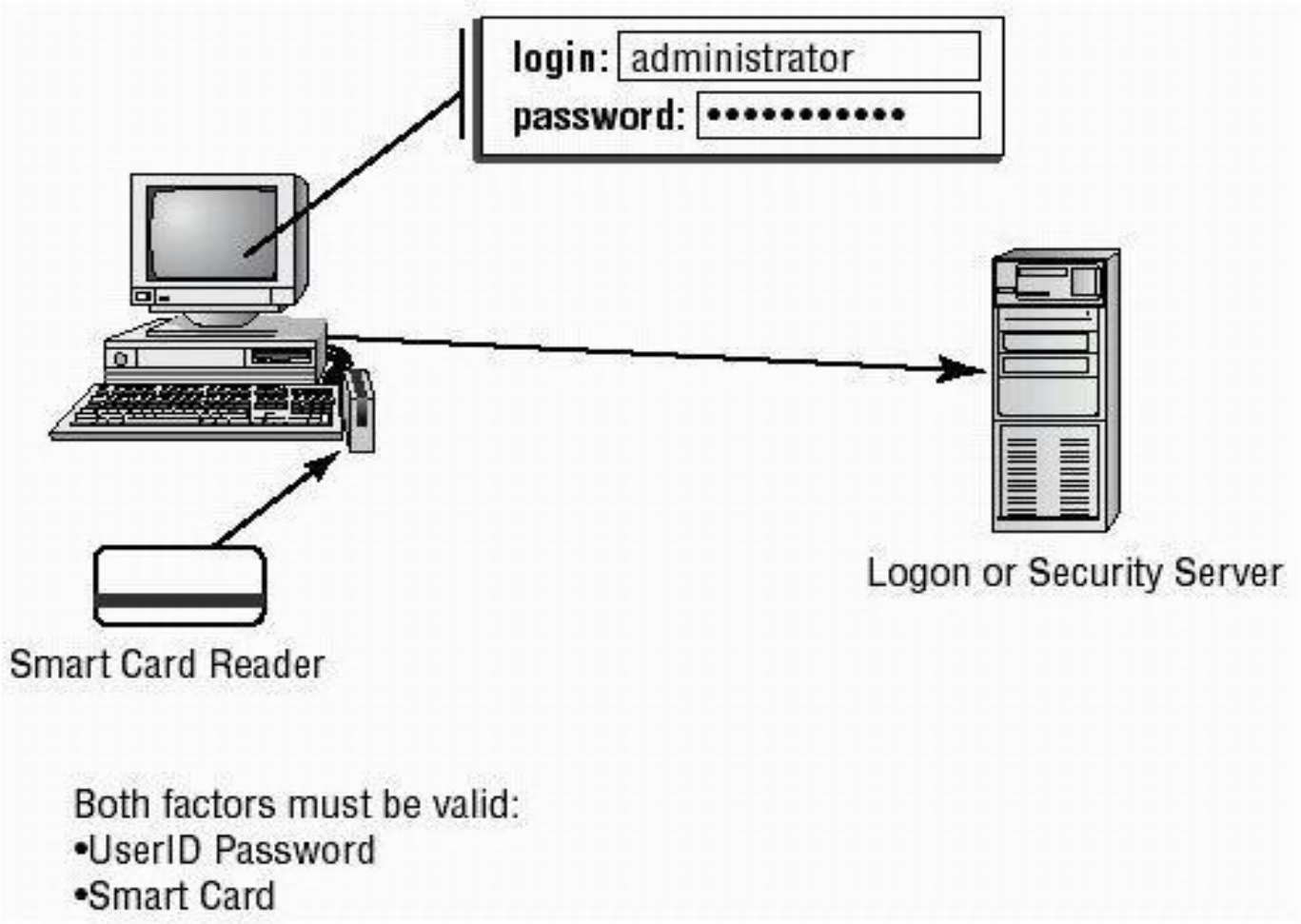
Phương pháp Kerberos :

Kerberos cho phép một đăng nhập đơn vào mạng phân tán.

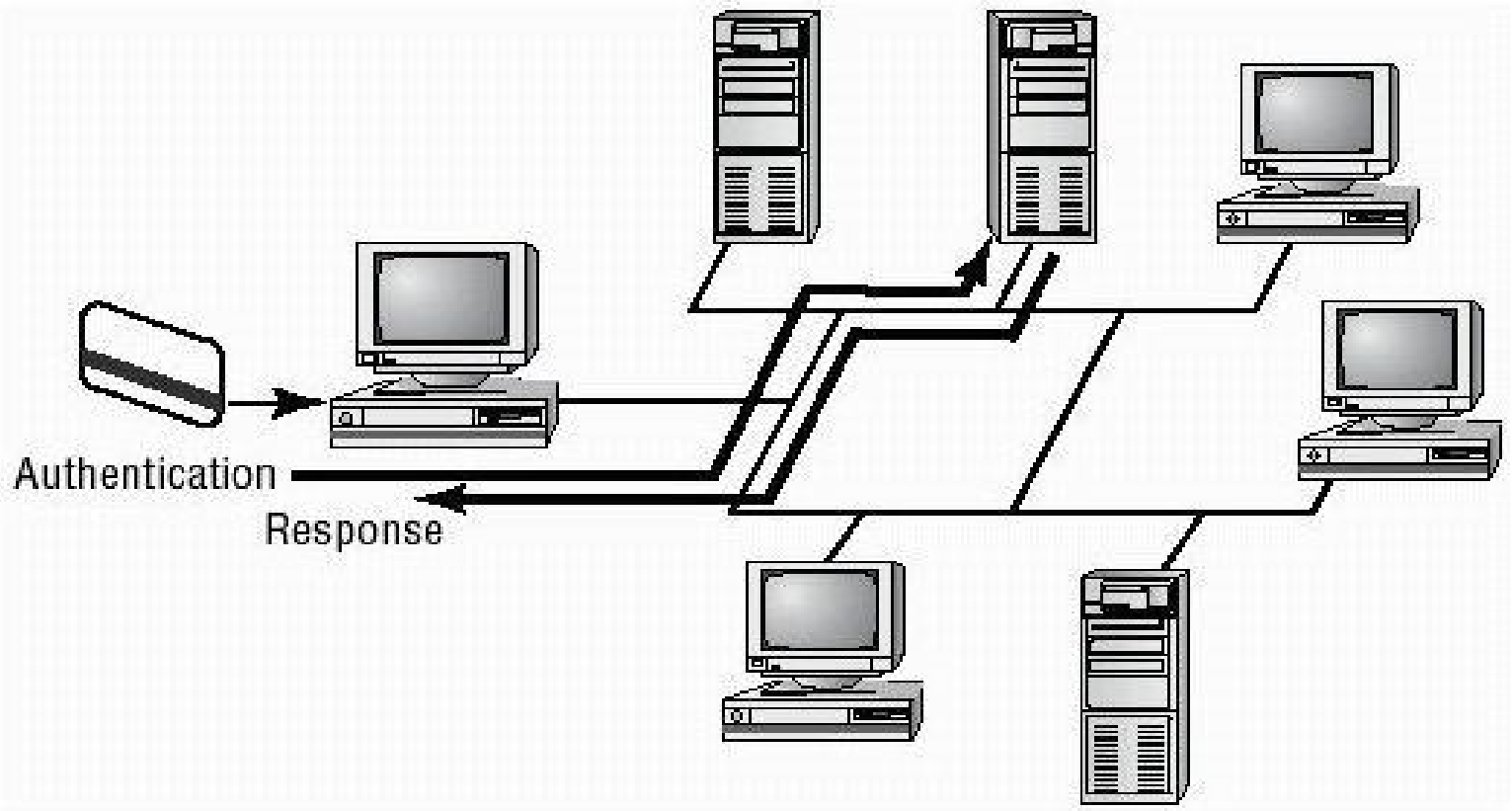


1. User requests access to service running on a different server.
2. KDC authenticates user and sends a ticket to be used between the user and the service on the server.
3. User's workstation sends ticket to service to authenticate and use the requested service.

Chứng thực đa yếu tố:



Chứng thực bằng thẻ thông minh (Smart card):



Chứng thực bằng sinh trắc học :

- Nhận dạng cá nhân bằng các đặc điểm riêng biệt của từng cá thể.
- Hệ thống sinh trắc học gồm các thiết bị quét tay, quét võng mạc mắt, và sắp tới sẽ có thiết bị quét DNA
- Để có thể truy cập vào tài nguyên thì bạn phải trải qua quá trình nhận dạng vật lý

Những vấn đề thực tế

- Phù hợp với trình độ và năng lực của nhân viên và hệ thống.
- Không nên tiêu tốn nhiều thời gian và tiền bạc vào những hệ thống an toàn phức tạp khi chưa có một chính sách an toàn phù hợp.
- Hãy cẩn thận với khuynh hướng sử dụng những username thông dụng và những mật khẩu dễ đoán như :”123” hoặc “ abcd”…
- Sử dụng chứng thực và đảm bảo an toàn đa yếu tố gồm một thẻ thông minh và mật khẩu.

- *Có rất nhiều vần đề khác phải quan tâm,đó là:*

✓ Tính dễ bị tấn công của hệ thống .

✓ Các điểm yếu của hệ thống.

✓ Không tương xứng của những chính sách an toàn.

✓ Vấn đề kết nối Internet :Khi mạng kết nối với Internet thì nó sẽ trở thành một đối tượng tiềm năng cho các cuộc tấn công .

7.3. Quản trị và các chính sách

- Cung cấp những hướng dẫn, những quy tắc , và những quy trình để thiết lập một môi trường thông tin an toàn .
- Để những chính sách bảo mật phát huy hết hiệu quả thì ta phải có ***sự hỗ trợ toàn diện và triệt để từ phía các nhà quản lý trong tổ chức.***

Một số chính sách quan trọng

- Chính sách nhà quản trị
- Yêu cầu thiết kế
- Kế hoạch khôi phục sau một biến cố
- Chính sách thông tin
- Chính sách an toàn
- Chính sách về cách sử dụng
- Chính sách quản lý người dùng

a.Chính sách nhà quản trị

- Trình bày đường lối chỉ đạo và những quy tắc , quy trình cho việc nâng cấp, theo dõi, sao lưu, và kiểm toán (Audit) .

b.Nhu cầu thiết kế

- Khả năng cần phải có của hệ thống để đối phó với các rủi ro về an toàn . Những nhu cầu này là rất căn bản trong phần thiết kế ban đầu và nó có ảnh hưởng rất lớn đến các giải pháp được sử dụng
- Những chính sách này mô tả thật rõ ràng về các nhu cầu bảo mật

c.Kế hoạch khôi phục sau biến cố (DRP- Disaster Recovery Plans)

- Một trong những vấn đề nhức đầu nhất mà các chuyên gia CNTT phải đối mặt
- Tốn rất nhiều tiền để thực hiện việc kiểm tra,sao lưu,thiết lập hệ thống dự phòng để giữ cho hệ thống hoạt động liên tục.
- Hầu hết các công ty lớn đều đầu tư một số tiền lớn vào kế hoạch khôi phục bao gồm việc sao lưu dữ liệu hay những lập“điểm nóng”.
- “Điểm nóng” là một nơi được thiết kế để cung cấp các dịch vụ nhanh chóng và thuận tiện nhất khi có sự cố xảy ra như hệ thống hay mạng bị sập.

d.Chính sách thông tin

- Truy suất, phân loại, đánh dấu và lưu trữ, dự chuyển giao hay tiêu huỷ những thông tin nhạy cảm.
- Sự phát triển của chính sách thông tin là sự đánh giá chất lượng an toàn thông tin.

e. Chính sách bảo mật

- Cấu hình hệ thống và mạng tối ưu : cài đặt phần mềm, phần cứng và các kết nối mạng.
- Xác định và ủy quyền. Định rõ việc điều khiển truy cập, kiểm toán, và kết nối mạng.
- Các phần mến mã hóa và chống virus được sữ dụng để thực thi những chính sách này.
- Thiết lập các chức năng hay các phương thức dùng để lựa chọn mật mã, sự hết hạn của mật mã, nổ lực truy cập bất hợp pháp và những lĩnh vực liên quan.

f.Chính sách về sử dụng

- Thông tin về nguồn tài nguyên được sử dụng như thế nào với mục đích gì?
- Những quy định về cách sử dụng máy tính: đăng nhập , mật khẩu,an toàn vật lý nơi làm việc…
- Những quy định về sự riêng tư, quyền sở hữu và những hậu quả khi có những hành động không hợp pháp.
- Cách sử dụng Internet và Email.

g. Quản lý người dùng

- Các định các thao tác được thực hiện ở những trường hợp bình thường trong hoạt động của nhân viên.
- Cách ứng xử với các nhân viên mới được kết nạp thêm vào hệ thống.
- Hướng dẫn và định hướng cho nhân viên,điều này cũng quan trọng tương tự như khi ta cài đặt và cấu hình một thiết bị mới.

Mục đích của an toàn thông tin

- Mục đích của ATTTnói ra rất dễ nhưng thực hiện nó thì không đơn giản.
- Mục đích của an toàn thông tin rất rõ ràng và nó được lập thành một bộ khung để có thể căn cứ vào đó phát triển và duy trì một kết hoạch bảo vệ an toàn thông tin

Mục đích:

a. Phòng ngừa :

- Nhằm ngăn chặn các hành động xâm phạm máy tính hay thông tin một cách phạm pháp.
- Thiết lập các chính sách và các chức năng của hệ thống an toàn nhằm giảm thiểu nguy cơ bị tấn công
- Chính sách ngăn chặn càng tốt thì mức thành công của các cuộc tấn công càng thấp

b. Phát hiện :

- Xác định các sự kiện khi nó đang thực hiện. Trong nhiều trường hợp việc phát hiện này rất khó thực hiện
- Để phát hiện có thể sử dụng một vài công cụ đơn giản hoặc phức tạp hay chỉ là việc kiểm tra các logfile
- Thực hiện liên tục
- Là một phần trong chính sách và chức năng bảo đảm an toàn thông tin của bạn.

c. Đáp trả

- Phát triển các chiến lược và kỹ thuật để có thể giải quyết các cuộc tấn công hay mất mát dữ liệu
- Việc phát triển một hệ thống đáp trả thích hợp bao gồm nhiều yếu từ đơn giản đến phức tạp
- Nên có những chức năng và phương thức cho việc khôi phục lại sau khi bị tấn công hơn là cố gắng tạo ra những cái cao siêu.

1.6.Các dịch vụ và các giao thức

- Mỗi dịch vụ và giao thức được sử dụng sẽ làm tăng tính dễ bị tấn công của hệ thống và làm cho xuất hiện các vấn đề tiềm năng về an ninh trong hệ thống.
- Hàng ngày người ta tìm được những lổ hỗng mới cho các dịch vụ và giao thức được sử dụng phổ biến trong hệ thống mạng máy tính.

Các giao thức và dịch vụ thông dụng:

- Mail : Không an toàn
- Web : Không an toàn
- Telnet : Không được bảo vệ
- FTP –Không có mã hoá → S/FTP
- NNTP-Network News Tranfer Protocol
- DSN-Domain Name Service → DNS attack
- ICMP : Ping → không an toàn

Những giao thức và dịch vụ không thiết yếu

- Dịch vụ NetBIOS
- UNIX RPC
- NFS
- X Services
- R Services, ví dụ như rlogin, rexec
- Telnet
- FTP
- TFTP (Trivial File Tranfer Protocol)
- Netmeeting
- Remote Control System)
- SNMP (Simple Network Management Protocol)

1.7.An toàn Topology mạng

Xác định trong quá trình thiết kế và thực thi mạng

Bốn nội dung chính cần quan tâm

- Mục đích của thiết kế
- Vùng bảo mật
- Topology mạng
- Những yêu cầu kinh doanh

a. Mục đích của thiết kế

Mục đích : Đảm bảo tính bí mật, tính toàn vẹn, tính hiệu lực, và khả năng chịu trách nhiệm

- Tính bí mật : Ngăn cản hay hạn chế truy cập trái phép hoặc tiết lộ bí mật thông tin, dữ liệu
- Tính toàn vẹn: Đảm bảo dữ liệu đang làm việc không bị thay đổi so với với dữ liệu gốc
- Tính sẵn sàng: Đảm bảo hệ thống sẵn sàng đối phó với mọi tình huống
- Chịu trách nhiệm :Ai chịu trách nhiệm trước mọi hoạt động của hệ thống

b. Vùng bảo mật

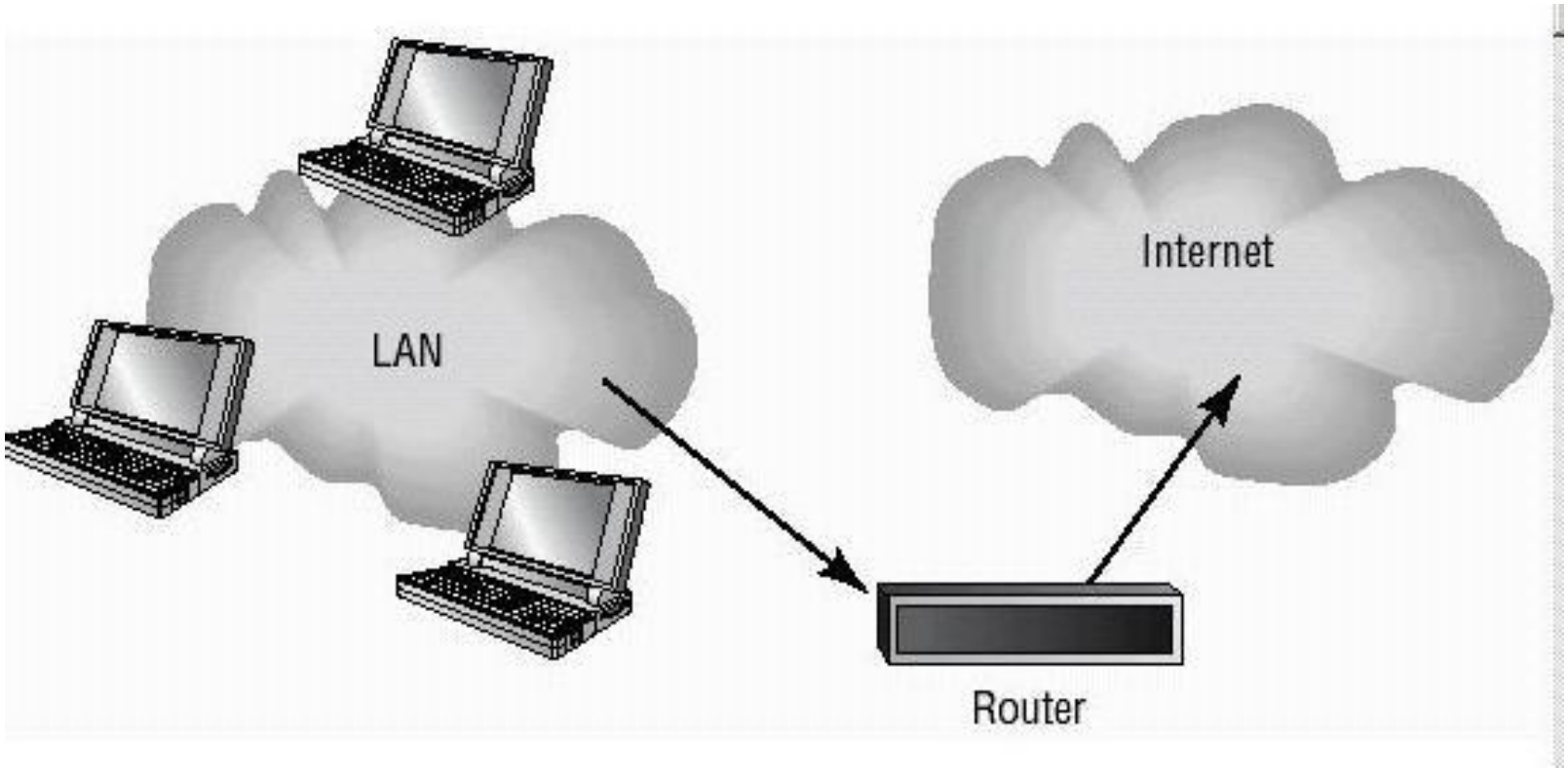
- Cách ly hệ thống của chúng ta với những hệ thống hay mạng khác
- Cách ly hệ thống khỏi những người truy cập không hợp lệ
- Là một nội dung quan trọng khi thiết kế mạng

Tổng quan về mạng :

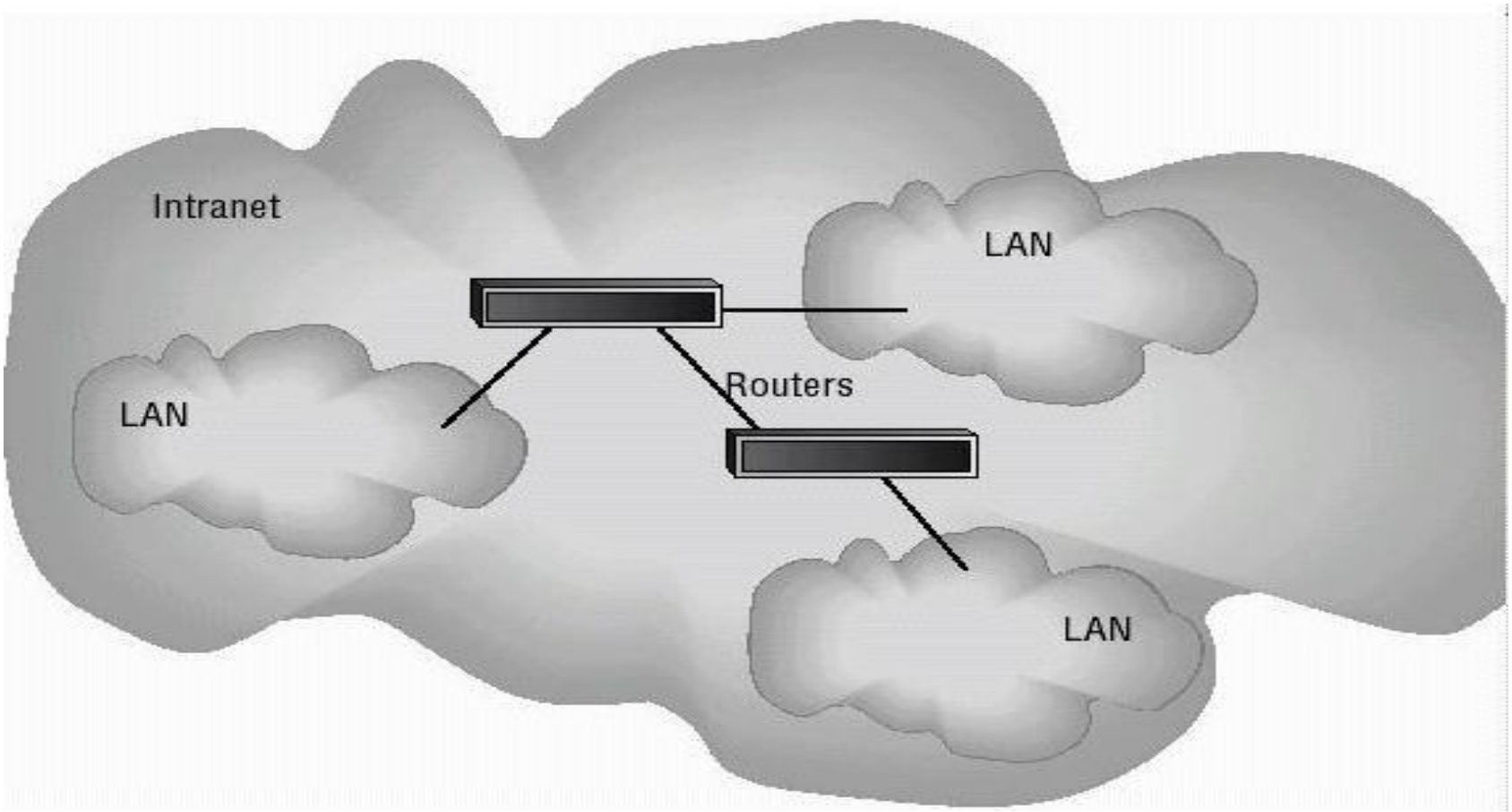
Bốn vùng bảo mật thông dụng:

- Internet
- Intranet
- Extranet
- DMZ (Demilitarized Zone – khu phi quân sự)

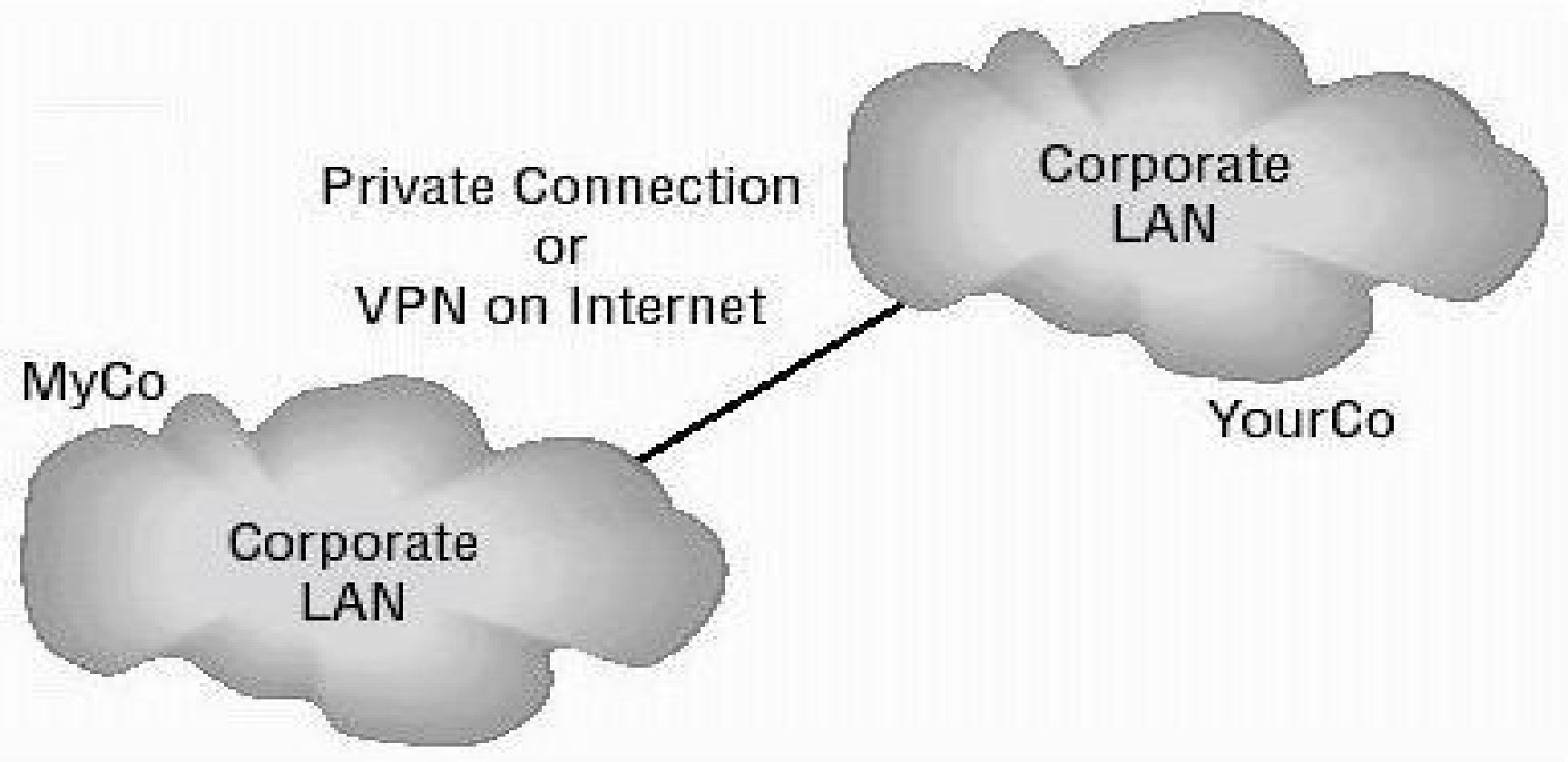
Internet



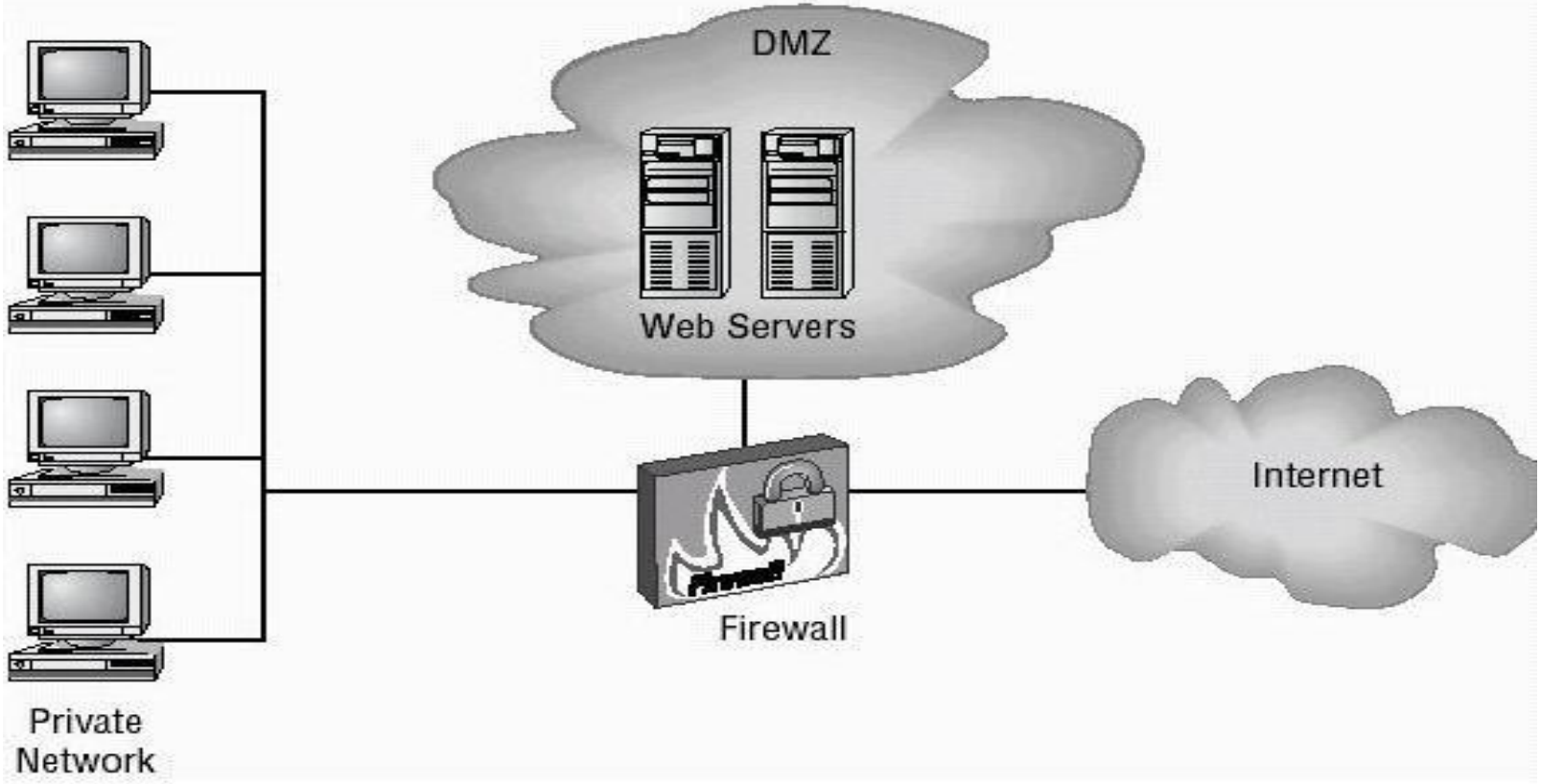
Intranet



Extranet

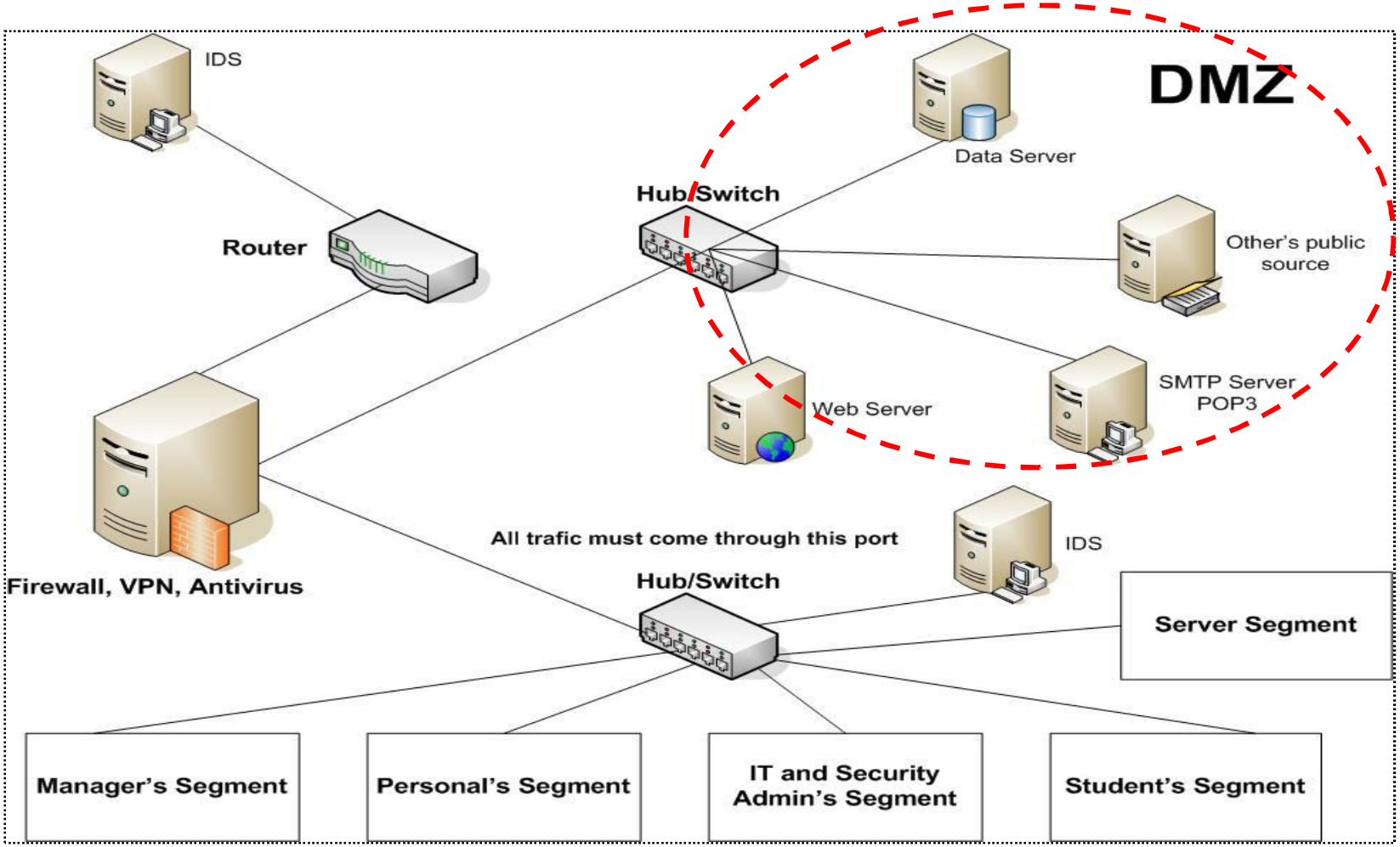

Private Connection
or
VPN on Internet
Corporate
LAN
MyCo
YourCo
Corporate
LAN

DMZ : *Dùng để đặt một máy chủ công cộng , mọi người có thể truy cập vào*



Thiết kế vùng bảo mật

Mô hình mẫu :

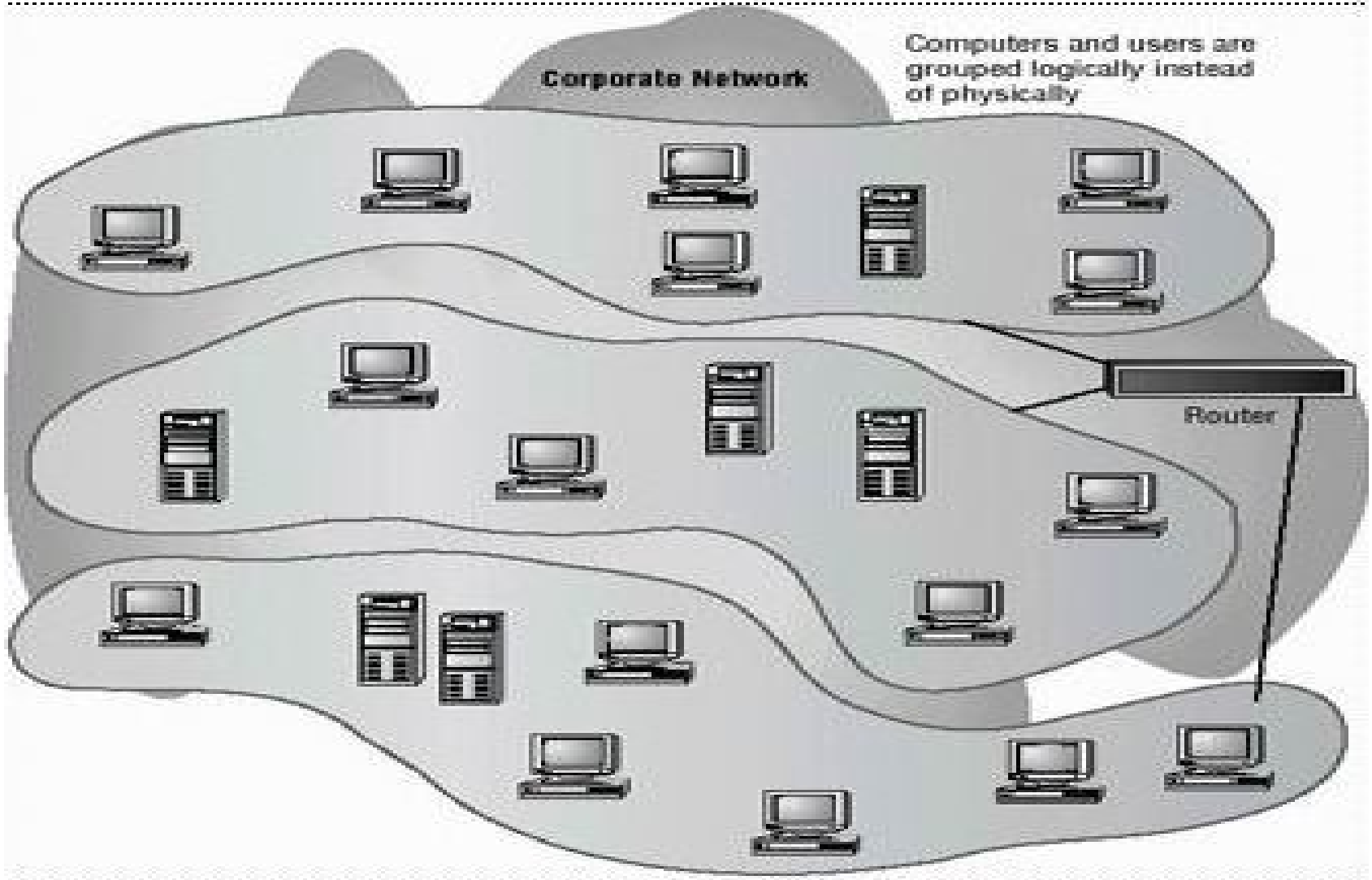


c. Thiết kế vùng bảo mật :

Công nghệ: VLAN , NAT, Tunneling

- VLAN : Cho phép dấu các segment để những segment khác không thấy được
- Kiểm soát được các truy cập trong các segment
- NAT : Network Address Transfer
- Tunneling : Vitual Private Network

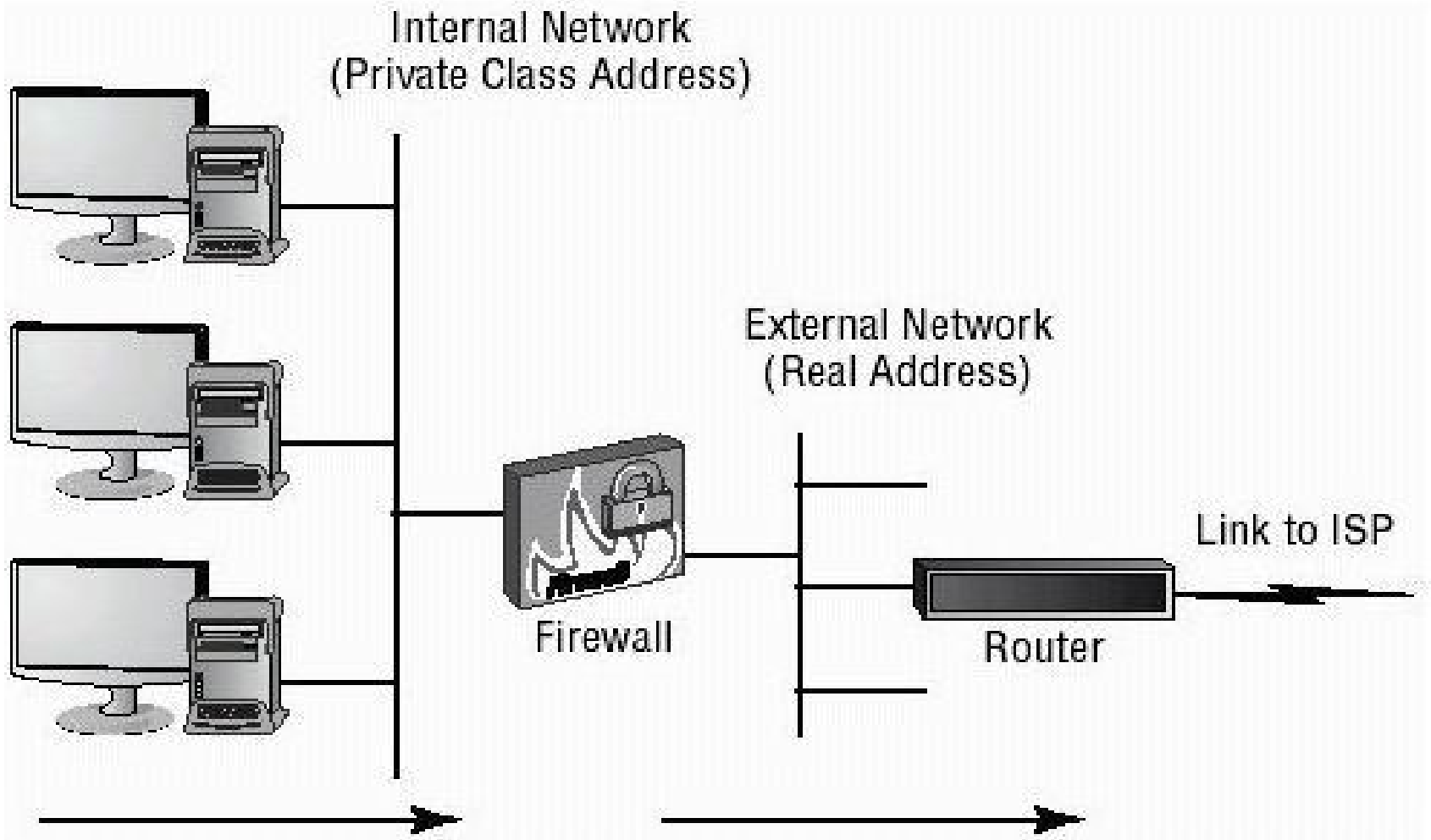
VLAN


Corporate Network
Computers and users are grouped logically instead of physically
Router

NAT

- Cung cấp khả năng duy nhất để truy nhập vào hệ thống mạng được bảo vệ
- NAT cho phép dùng một địa chỉ đơn để hiển thị trên Internet thay cho các địa chỉ trong mạng cục bộ
- Máy chủ NAT cung cấp các địa chỉ IP cho các máy chủ hay các hệ thống trong mạng, và nó ghi lại các lưu thông ra vào mạng
- Dùng NAT để đại diện cho tất cả các kết nối trong mạng cục bộ qua một kết nối đơn

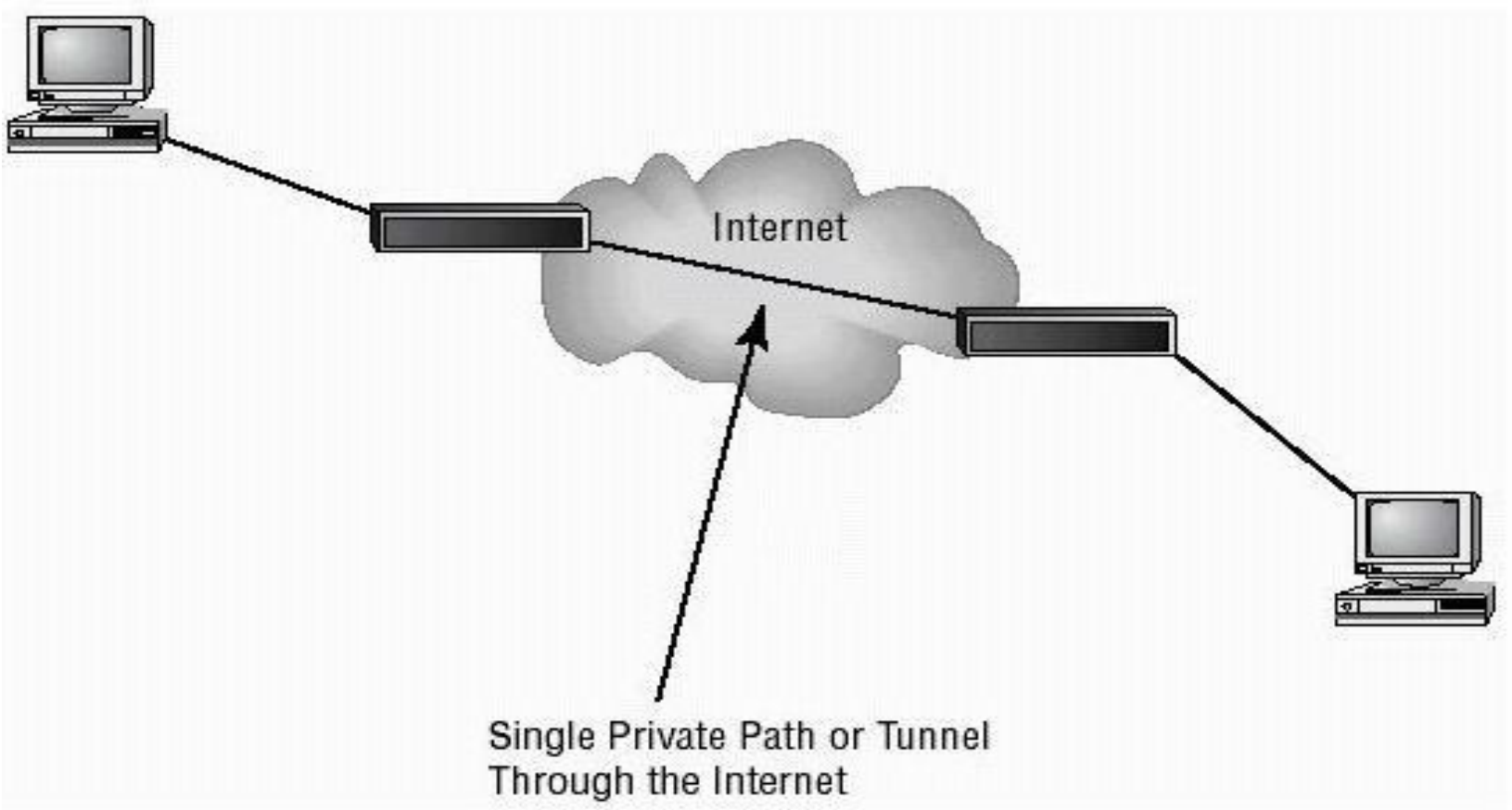
NAT


Internal Network
(Private Class Address)
External Network
(Real Address)
Link to ISP
Firewall
Router

Tunneling

- Đường hầm là khả năng tạo ra một kết nối ảo giữa hai hệ thống hay giữa hai mạng.
- Đường hầm được tạo giữa hai điểm cuối bằng cách đóng gói dữ liệu trong một giao thức truyền tin với sự thoả thuận của hai bên.
- Sử dụng mật mã giúp giao thức tunel có khả năng bảo vệ dữ liệu một cách an toàn (VPN)

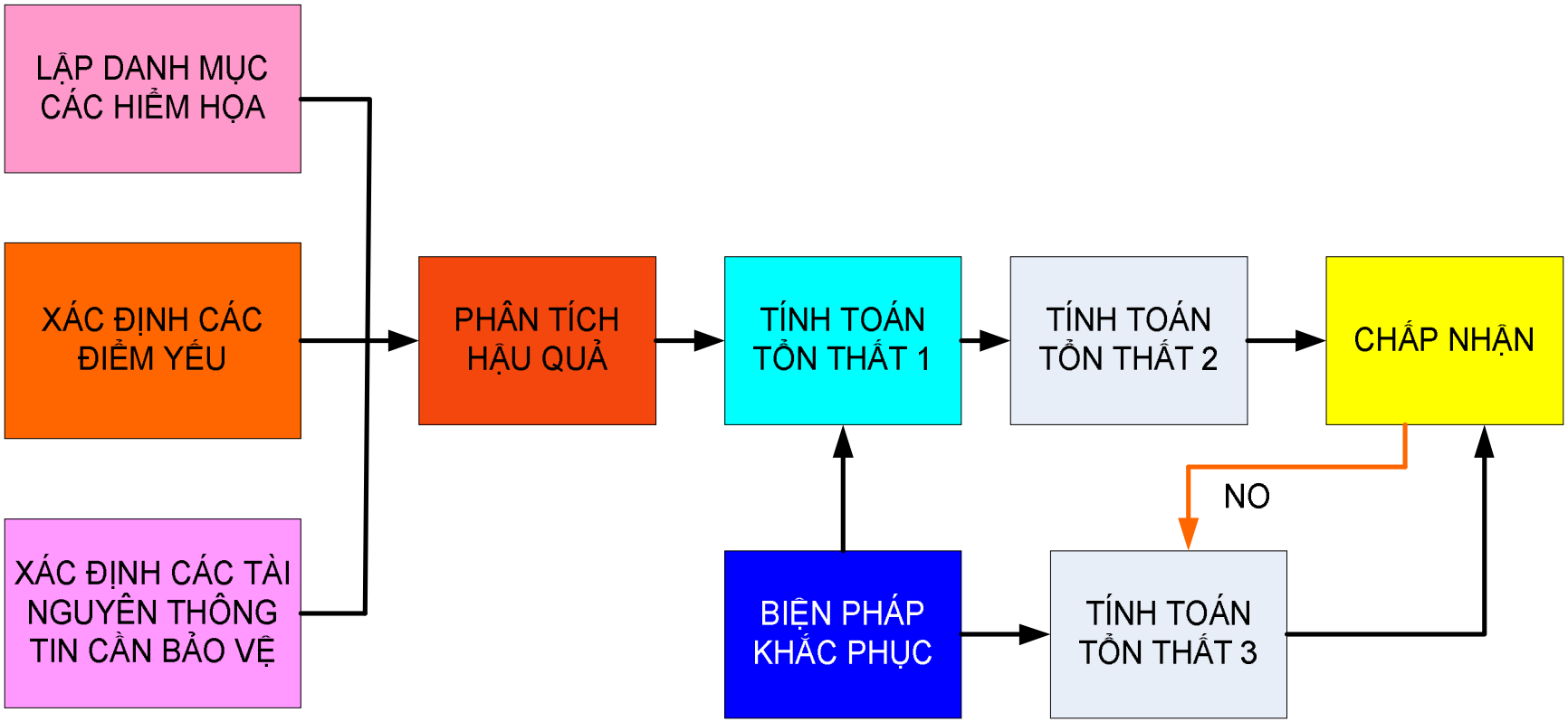
Tunneling


Internet
Single Private Path or Tunnel
Through the Internet

9.QUẢN LÝ RỦI RO

- Xác định rủi ro , sử dụng các giải pháp bảo vệ nhằm giảm thiểu rủi ro và xác định độ rủi ro có thể chấp nhận được (rủi ro dư thừa) trong hệ thống.
- Đánh giá tổn thất có thể xảy ra trong quá trình sử dụng hoặc phụ thuộc vào hệ thống TT
- Phân tich các mối đe dọa tiềm năng và các điểm yếu co thể gây tổn thất cho HTTT.
- Lựa chọn các giải pháp và các phương tiện tối ưu nhằm giảm thiểu rủi ro đến mức độ cho phép.

QUY TRÌNH PHÂN TÍCH RỦI RO

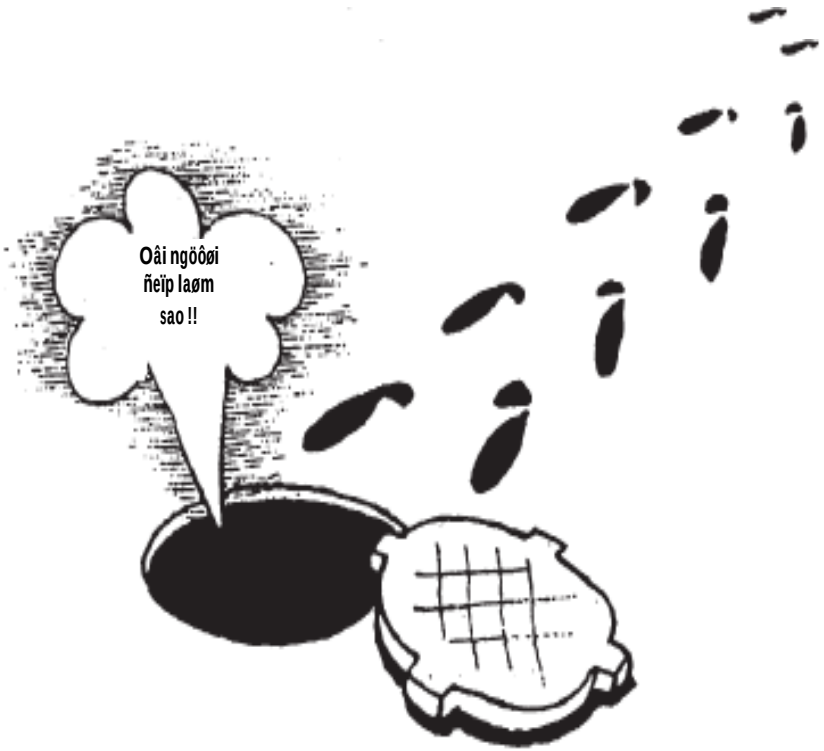


Những vấn đề cần giải quyết :

- Giá trị của thông tin (value of information) : ***Cần phải bảo vệ cái gì ?*** Lưu ý : Không phải bảo vệ tài nguyên (resource) mà là bảo vệ thông tin .
- Các mối đe dọa (hiểm họa) : TT có giá trị ***cần được bảo vệ khỏi cái gì ?*** và xác xuất tác động của hiểm họa.
- Tác động : Loại tác đông nào sẽ phá hoại thông tin khi xảy ra hiểm họa – ***tác động ở đâu , như thế nào ?*** :

  VD : Lộ thông tin , thay đổi thông tin trong quá trình trao đổi TT…
- Hậu quả : ***Hậu quả xảy ra*** khi hiểm họa : VD khi thụt hố ga sẽ bị gãy chân.
- Biện pháp khắc phục hiểm họa .
- Rủi ro tồn đọng : Múc rủi ro sau khí đưa ra các giải pháp bảo vệ , có chấp nhận hay không mức rủi ro này.

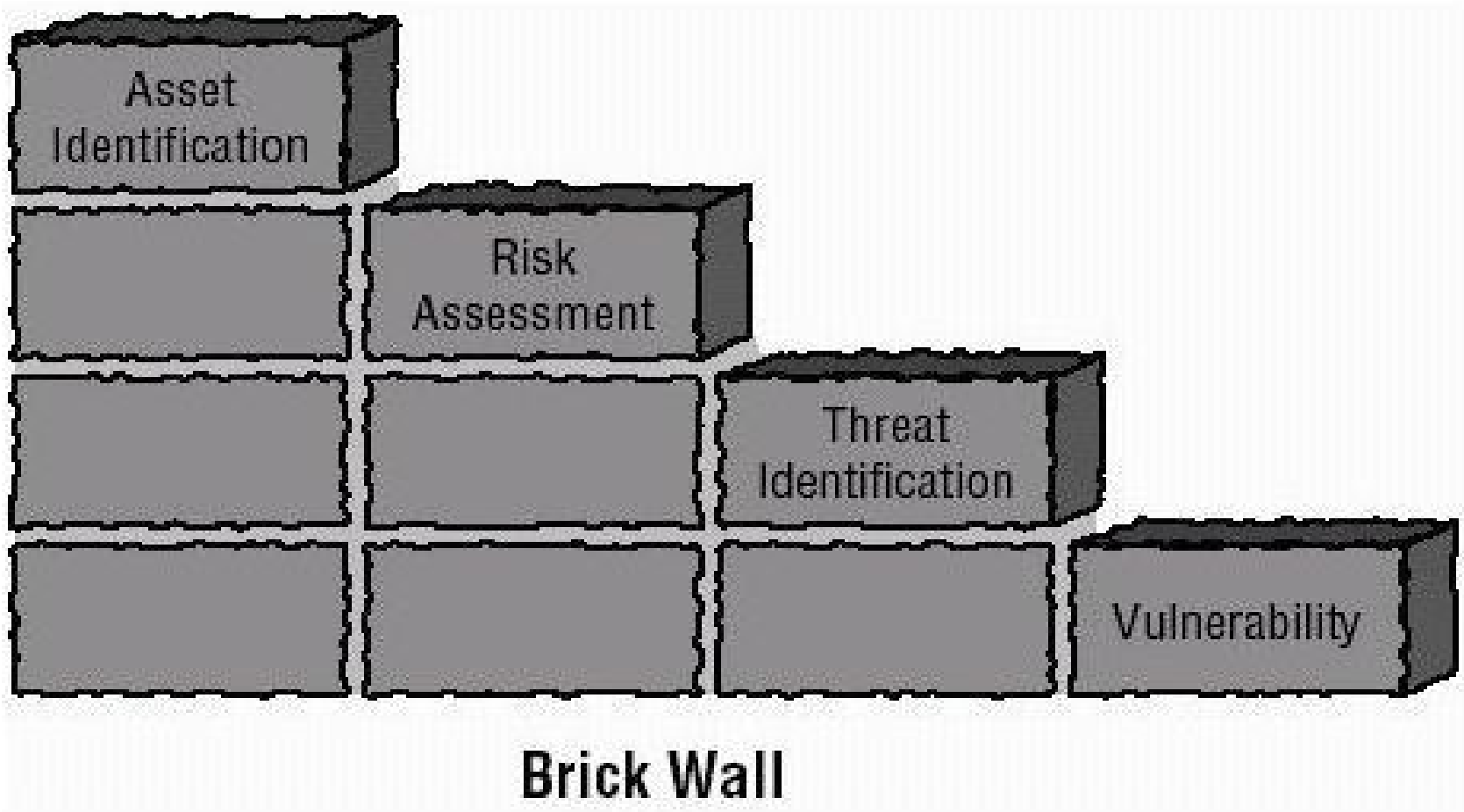
- ***Trên đường có hố ga không đậy nắp → Hiểm họa***
- ***Có người bị thụt hố → rủi ro → Xác xuất ? Ảnh hưởng của các hiểm họa khác "Mải nhìn người đẹp"***
- ***Bị va đập vào đầu → tác động***
- ***Chấn thương sọ não , tử vong → Hâu quả***
- ***Đậy nắp hố ga lại → Biện pháp***
- ***Nắp hố ga có đảm bảo không ? (độ dày ,kết cấu…) → rủi ro tồn đọng → Chấp nhận hay không?***



Mối lo lắng của doanh nghiệp

- Hiểu rõ về tình trạng an toàn của tổ chức?
- Bắt đầu từ đâu ? Câu trả lời không đơn giản
- Phải làm gì ? : Xác định tài sản, đánh giá toàn diện về rủi ro, xác định các mối đe dọa, tiên liệu các khả năng bị tấn công , các chính sách an toàn…
- Giúp cho giám đốc hiểu được họ đang đối mặt với những vấn đề gì, hiệu quả như thế nào nếu tập trung giả quyết các yếu tố này

Mối lo lắng của doanh nghiệp



1.Xác định tài sản :

- Mỗi doanh nghiệp hay tổ chức điều có những tài sản hay tài nguyên có giá trị.
- Các tài sản phải được kiểm toán cả về mặt vật lý lẫn chức năng.
- Quá trình xác định tài sản là quá trình đánh giá giá trị của các thông tin và hệ thống tại một nơi cụ thể.
- Sự ước lượng các loại tài sản vật lý là một quá trình kiểm toán thông thường mà một doanh nghiệp phải làm.

Xác định tài sản

- Xác định giá trị thông tin
- Xác định chức năng của nó và các thức tiếp cận thông tin
- Dễ dàng hơn trong việc đưa ra các phương án sự bảo vệ cho thông tin đó.

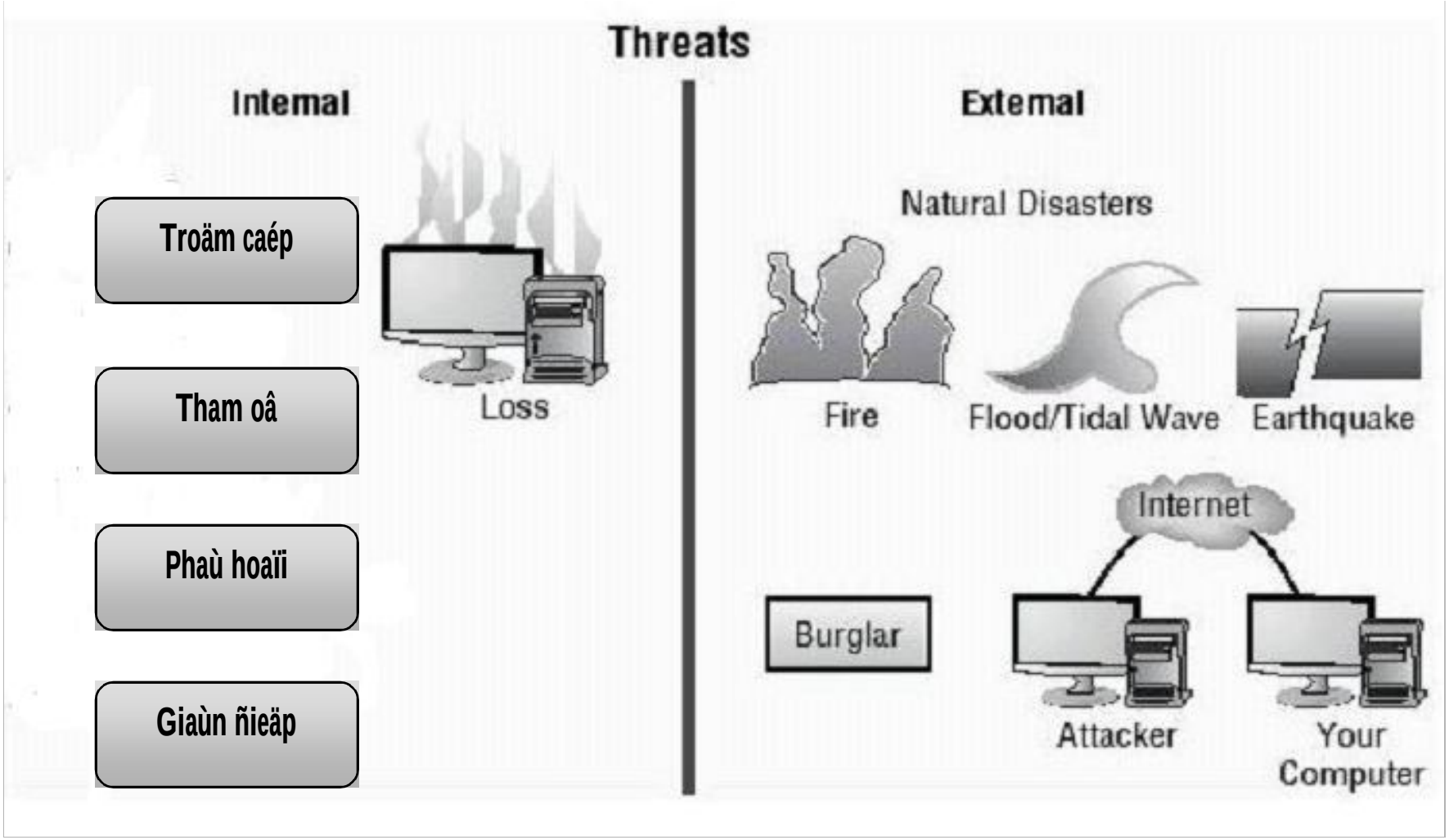
2.Đánh giá phân tích về rủi ro

- Có nhiều cách đánh giá hay phân tích những rủi ro.
- Việc đánh giá và phân tích rủi ro này được sắp xếp từ những phương thức khoa học cho đến việc đàm phán với người sở hữu thông tin.
- Phải xác định được chi phí cần thiết cho việc thay thế những dữ liệu và hệ thống bị đánh cắp, chi phí cho thời gian ngừng, hay tất cả những gì mà ta có thể tưởng tượng ra được đối với các rủi ro.

3.Xác định hiểm hoạ

- Phải tiên liệu được các các mối đe dọa bên trong và bên ngoài đối với mạng và dữ liệu.
- Thật chẳng hiệu quả nếu ta cung cấp một môi trường bảo vệ công ty khỏi các mối đe dọa bên ngoài trong khi hầu hết các đe dọa đều xuất từ bên trong
- Hiểm hoạ từ bên trong có thể là nhân viên giả dạng, sự lạm dụng quyền hạn, sự thay đổi dữ liệu và đánh cắp tài sản → một nguy cơ tiềm ẩn.

Các hiểm nguy



Các mối đe dọa từ bên trong :

- Gây nhiều tác hại nhất : Chiếm 70%
- Điều quan trọng là biết cách tìm ra và cách loại các mối đe dọa bên trong, đây là mấu chốt trong công việc bảo mật thông tin máy tính.

Các mối đe dọa từ bên ngoài

- Các mối đe dọa từ bên ngoài đang tăng với tốc độ báo động.
- Sử dụng trực tuyến cơ sở dữ liệu, giao dịch tài chính , chi trả tiền lương, ký gửi hàng hóa , kiểm kê, và các thông tin quản lý quan trọng khác .
- Kết nối với những hệ thống thông tin hợp tác, bí mật thương mại, và rất nhiều thông tin giá trị khác.

Phương thức tấn công dễ dàng

- Những công cụ tự động tìm kiếm mục tiêu và tấn công vào hệ thống thông qua những lỗ hổng của nó.
- Có rất nhiều công cụ tấn công . Không cần phải là một chuyên gia về kỹ thuật cũng có thể trở thành một hacker.
- Có rất nhiều hệ thống máy tính bị tấn công nhiều lần bằng những phương thức giống nhau do những kẻ tò mò thực hiện hay những tội phạm đang cố thực hiện hành động phạm pháp của mình.

9 .Nhiệm vụ của quản trị an toàn mạng (Chief Security Officer)

- Dự báo , phân tích các rủi ro
- Phòng ngừa
- Phát hiện các cuộc tấn công
- Chống trả
- Hỗ trợ cho các nhân viên pháp luật điều tra

Những nơi dễ bị tấn công

- Sử dụng username và password
- Giao thức TCP/IP
- Các phần mềm có giao diện đồ họa, dễ dàng cấu hình → nảy sinh vấn đề bảo mật
- Email cho phép đính kèm các file thực thi.

Kết thúc chương 1