HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA ATTT

BÀI GIẢNG PTTK AN TOÀN MẠNG

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

Mục tiêu giai đoạn phân tích

- Mục tiêu của giai đoạn phân tích là cung cấp một giải pháp thực tế đối với vấn đề đặt ra trong giai đoạn khảo sát.
- Phải xác định khả năng có thể thiết kế và cài đặt những yêu cầu an toàn và điều chỉnh phù hợp tuân theo ngân sách, tài nguyên và ràng buộc thời hạn hoàn thành.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Xác định và phân tích các mục tiêu cơ bản
  - Phân tích mục tiêu thương mại
  - Phân tích mục tiêu kỹ thuật
  - Xác định các đặc tính mạng hiện có
  - Kiểm tra khả năng hoạt động của mạng
  - Xác định lưu lượng mạng
- Xác định và phân tích các yêu cầu an toàn
  - Xác định giá trị tài sản mạng
  - Phân tích rủi ro
  - Xác định các yêu cầu an toàn

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.1 Phân tích mục tiêu hoạt động

- **Các mục tiêu thương mại cơ bản:**
  - Tăng doanh thu và lợi nhuận
  - Tăng thị phần
  - Mở rộng thị trường mới
  - Tăng cao tính cạnh tranh trong cùng thị trường
  - Giảm giá thành
  - Tăng năng suất lao động của nhân viên
  - Giảm thời gian vòng đời phát triển sản phẩm
  - Sử dụng trong thời gian cho phép
  - Đề xuất các dịch vụ mới cho khách hàng
  - Đề xuất các hỗ trợ mới tốt hơn cho khách hàng

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- **Các mục tiêu thương mại cơ bản :**
  - Kết nối các thành phần (Nhà đầu tư, khách hàng, đối tác, nhà cung cấp, nhân viên vv..)
  - Tránh sự gián đoạn hoạt động gây ra bởi các thảm họa tự nhiên và không tự nhiên
  - Hiện đại hóa các công nghệ đã lạc hậu
  - Làm cho trung tâm dữ liệu hiệu quả hơn trong việc sử dụng nguồn, cáp, rack, bộ nhớ và mạng WAN.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- **Danh sách các việc cần thực hiện:**
  - Hiểu được lĩnh vực hoạt động và cơ cấu tổ chức
  - Xác định được các ứng dụng mạng của khách hàng
  - Hiểu được chính sách của khách hàng đối với các nhà sản xuất thiết bị, phần mềm, giao thức, nền tảng hoạt động, chính sách đối việc thiết kế thực thi hệ thống vv..
  - Biết được chi phí và thời gian thực hiện dự án
  - Biết được trình độ chuyên môn kỹ thuật của khách hàng và các vấn đề liên quan
  - Nhận thức được vấn đề chính trị có thể ảnh hưởng đến việc thiết kế.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Xác định và phân tích các mục tiêu cơ bản
  - Phân tích mục tiêu hoạt động
  - **Phân tích mục tiêu kỹ thuật**
  - Xác định các đặc tính mạng hiện có
  - Kiểm tra khả năng hoạt động của mạng
  - Xác định lưu lượng mạng
- Phân tích và xác định các yêu cầu an toàn
  - Xác định giá trị tài sản mạng
  - Phân tích rủi ro
  - Xác định các yêu cầu an toàn

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.2 Mục tiêu kỹ thuật

- Khả năng mở rộng
- Tính sẵn sàng
- Hiệu năng mạng
- Quản lý mạng
- Khả năng tương thích

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.2 Phân tích mục tiêu kỹ thuật

3.1.2.1 Khả năng mở rộng

- Khi thiết kế phải tính toán đến khả năng mở rộng của mạng về quy mô mạng
- Nhiều công ty lớn bổ sung thêm người dùng, ứng dụng, các website, mở rộng kết nối mạng, tăng tốc độ mạng.
- Kế hoạch cho mở rộng: thiết kế mạng phải lên kế hoạch mở rộng mạng trong phạm vi 2 năm (hoặc 5 năm).

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Có thể sử dụng một danh sách các câu hỏi để phân tích những mục tiêu kỹ thuật cho việc mở rộng:
  - Có bao nhiêu website sẽ được thêm vào trong năm tới? hai năm tới?
  - Bao nhiêu người dùng sẽ truy cập vào trong mạng trong năm tới? hai năm tới?
  - Bao nhiêu server sẽ được thêm vào mạng công ty trong năm tới? hai năm tới?
  - Vv..

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.2.2 Tính sẵn sàng

- Tính sẵn sàng có thể được xem như phần trăm thời gian hoạt động trong một năm, một tháng, một tuần, một ngày, một giờ so với tổng số thời gian
- Trong một hệ thống thì tỷ lệ hoạt động của hệ thống tối thiểu phải đạt được 99.70%, Giá trị hướng tới 99.999%)

(Mạng chỉ bị down 5 phút trong một năm)

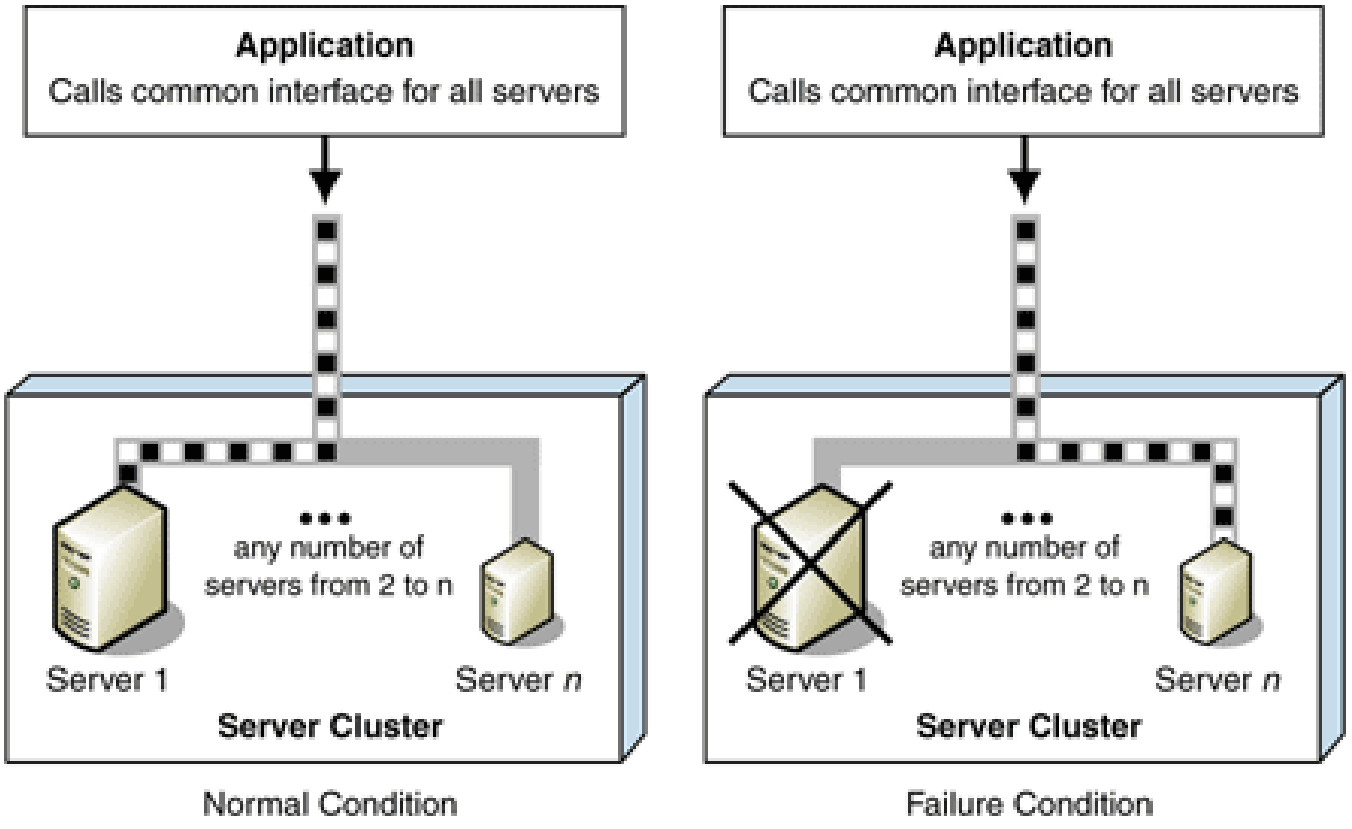
- Khả năng sẵn sàng tương ứng với vấn đề dự phòng (redundancy), nó là giải pháp để nâng cao khả năng sẵn sàng của mạng. Dự phòng có nghĩa là thêm liên kết hoặc thiết bị tới một mạng tương tự để tránh thời gian chết của mạng khi có sự cố xảy ra

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Dự phòng rất quan trọng khi muốn chắc chắn là hoạt động kinh doanh vẫn diễn ra bình thường khi xảy ra một sự cố hoặc thảm họa.
- Khả năng sẵn sàng cũng tương ứng với khả năng phục hồi (resiliency). Khả năng phục hồi là vấn đề đưa hoạt động mạng trở lại bình thường khi có các sự cố xảy ra như sự vi phạm an ninh, các thảm họa tự nhiên, lỗi của con người và lỗi phần mềm, phần cứng và hỏng hóc. Phần lớn các tổ chức cần có một kế hoạch để cho hoạt động kinh doanh và kỹ thuật diễn ra bình thường sau một thảm họa tự nhiên như lũ lụt, cháy, động đất, khủng bố…

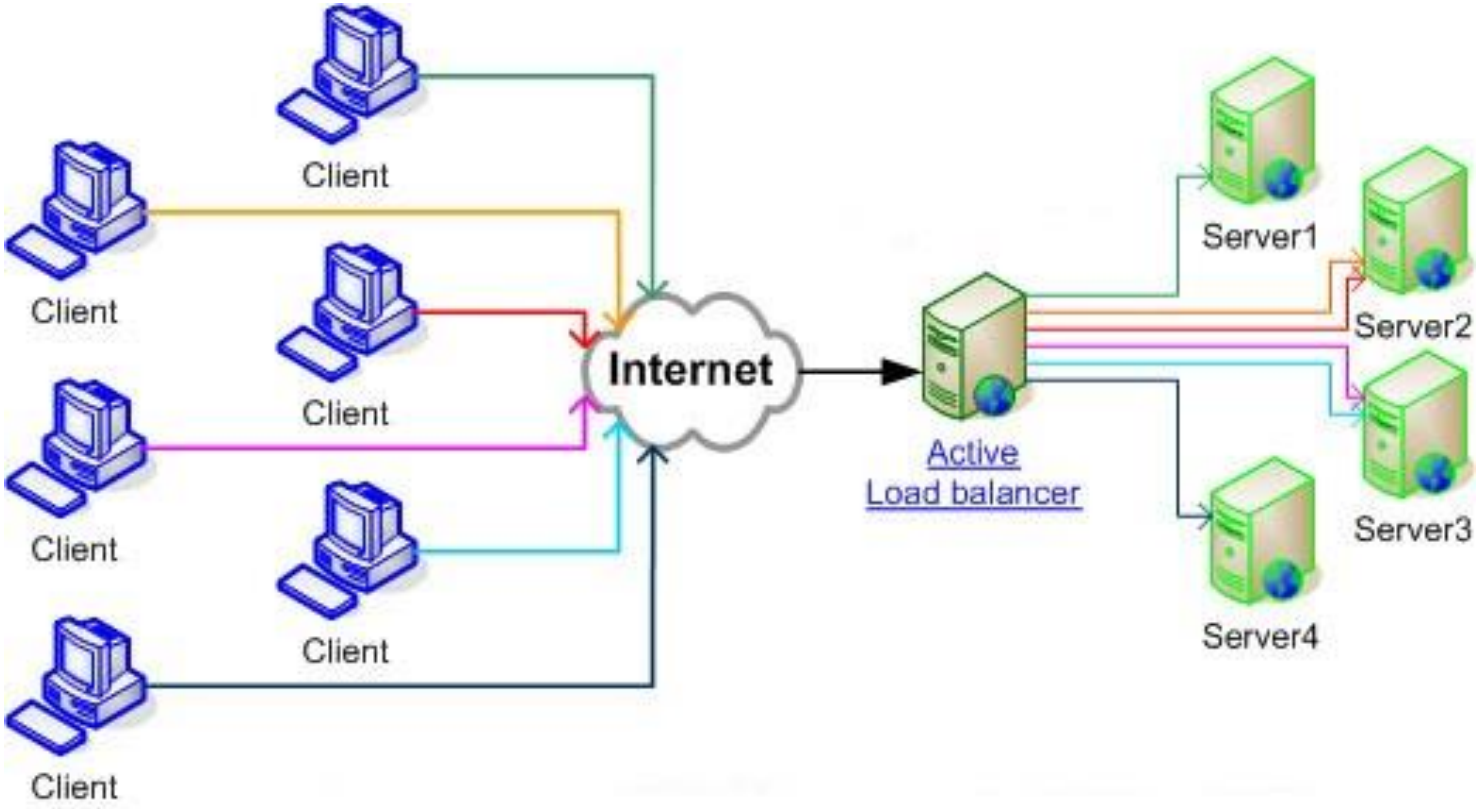
CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Công nghệ Clustering:



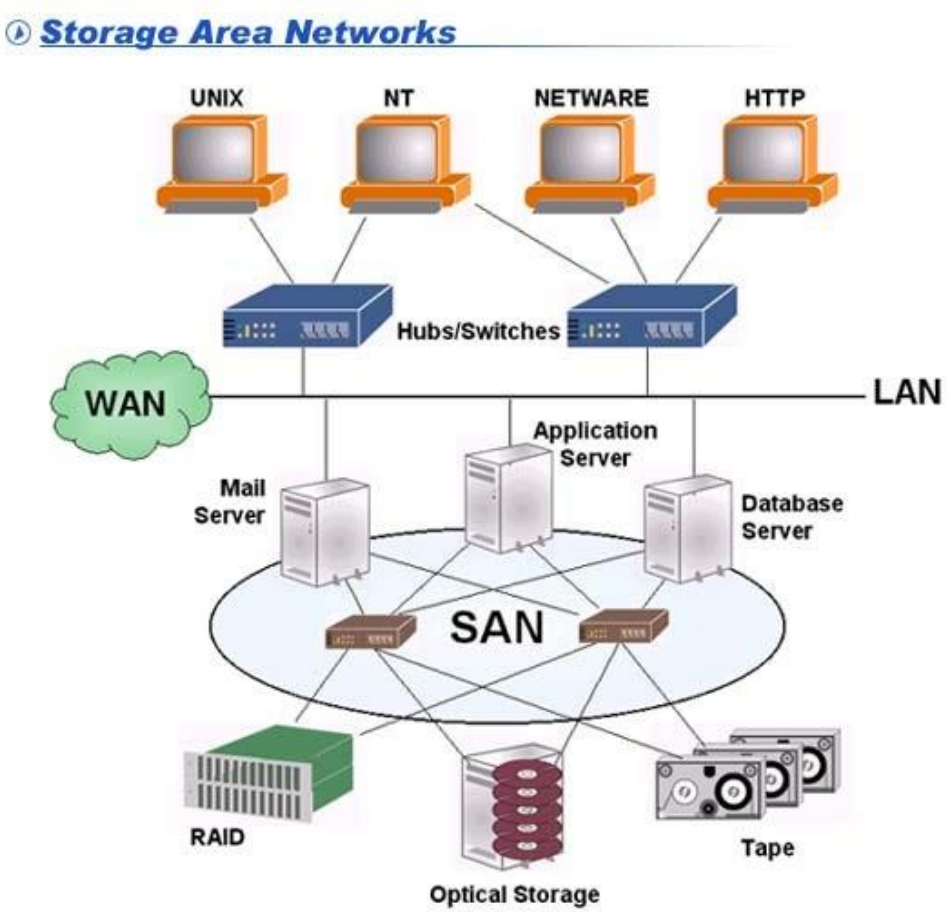
CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Công nghệ Load Balancing:



CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Công nghệ SAN:



CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.2.3 Hiệu năng mạng

- Khi phân tích những yêu cầu kỹ thuật cho thiết kế mạng, ta cần phân tích hiệu năng của mạng, nó bao gồm:
  - Bandwidth: khả năng vận chuyển dữ liệu của một mạch hoặc mạng, thường sử dụng số bit trên giây (bps)
  - Throughput: lượng dữ liệu được truyền tải thành công giữa 2 node trong một khoảng thời gian, thường là giây.
  - Delay: Thời gian giữa một frame được truyền từ một node và phân phối frame đó tới một nơi khác trong mạng.
  - Response time: Thời gian từ lúc yêu cầu một dịch vụ mạng cho đến khi được đáp ứng yêu cầu đó.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Mất gói dữ liệu tại các thiết bị liên mạng
- Nhân tố hiệu năng của máy chủ và máy trạm
  - Tốc độ truy cập đĩa
  - Kích cỡ bộ nhớ đệm
  - Hiệu năng trình điều khiển thiết bị
  - Hiệu năng của bus máy tính
  - Hiệu năng của CPU
  - Hiệu năng của bộ nhớ
  - Yếu tố hệ điều hành
  - Ứng dụng và các các lỗi của ứng dụng

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

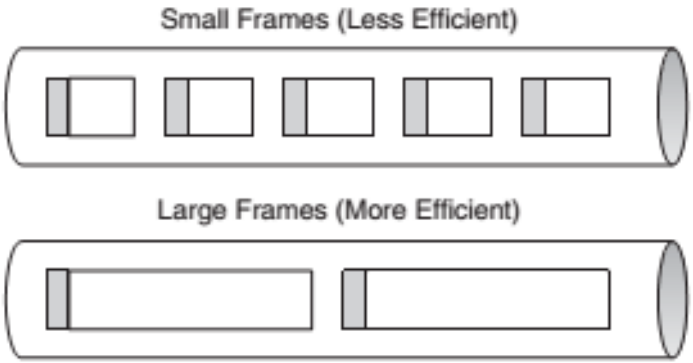
- Độ chính xác:
  - Đó là đề cập đến số các frame bị lỗi khi truyền trên tổng số các frame được truyền đi. Độ chính xác cũng có thể mô tả mức độ thường xuyên mạng sắp xếp lại trình tự của các gói dữ liệu.
  - Sự sắp xếp lại có thể xảy ra trong nhiều tình huống bao gồm cả việc sử dụng chuyển mạch song song trong các thiết bị mạng và sử dụng song song các liên kết giữa các thiết bị định tuyến
  - BER (WAN): Tỉ lệ lỗi bit: cáp quang: 1/10^11, dây đồng: 1/10^6

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Hiệu quả: là sự đánh giá hiệu quả của một thao tác khi so với công sức, năng lượng, thời gian hoặc chi phí bỏ ra.
  - Hiệu quả hệ thống mạng chỉ ra chi phí cần thiết để truyền một đơn vị dữ liệu, chi phí bị ảnh hưởng do tỉ lệ đụng độ, qua mã thông báo, báo cáo lỗi, thay đổi lộ trình, sự phản hồi, Frame có header lớn, một thiết kế mạng kém, vv
  - Mạng Ethernet chia sẻ là không hiệu quả khi mà tỉ lệ (collision) đụng độ cao

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Trong một số trường hợp người ta tối ưu thông lượng ứng dụng để tăng tính hiệu suất mạng thông qua sử dụng frame có kích thước lớn, đồng thời cũng tối ưu được băng thông



- Tuy nhiên khi Frame bị lỗi sẽ phải truyền lại gây ra tốn băng thông và giảm hiệu quả, do vậy người ta thường phải hạn chế kích cớ lớn nhất của 1 frame ví dụ đối với mạng Ethernet là 1522 bytes bao gồm cả header, CRC và và một thẻ VLAN 802.1Q

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.2.4 Quản lý mạng

- **Quản lý lỗi** (fault management): phát hiện, cách ly và xử lý vấn đề, báo cáo lỗi tới người dùng cuối và người quản trị.
- **Quản lý cấu hình** (configuration management): điều khiển, hoạt động, định danh và tập hợp dữ liệu từ thiết bị được quản trị.
- **Quản lý tài khoản** (accounting management): được sử dụng để cấp phát quyền tới người dùng mạng và thực hiện việc thay đổi yêu cầu người dùng.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- **Quản lý hiệu năng** (performance management): phân tích lưu lượng và hành vi ứng dụng để tối ưu mạng, xem xét các mức dịch vụ, lên kế hoạch cho việc mở rộng
- **Quản lý an toàn** (security management): quản lý, kiểm thử an toàn và chính sách bảo vệ, duy trì quản lý mật khẩu, thông tin xác thực, cấp quyền và quản lý phân phối khóa.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.2.5 Khả năng tương thích

- Một thiết kế mạng phải có khả năng tương thích với hệ thống mạng đã tồn tại từ trước nhằm giảm thiểu chi phí
- Giá cả phù hợp thường là mục tiêu chính, để tiết kiệm chi phí có thể sử dụng lại các thiết bị như switch, router…
- Trong mạng doanh nghiệp thì khả năng sẵn sàng thường quan trọng hơn là chi phí.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.3 Xác định các đặc tính mạng hiện có

- Tìm hiểu hạ tầng mạng hiện tại
  - Lập tài liệu phác họa sơ đồ mạng
  - Xây dựng một sơ đồ về các dịch vụ mạng
  - Lập tài liệu phác họa mô hình logic của mạng
- Tìm hiểu về tên và địa chỉ mạng
  - Đặc tính cơ sở hạ tầng mạng logic bao gồm tài liệu về việc đặt tên và địa chỉ của từng thiết bị mạng

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Đặc tính về dây và môi trường
  - Các loại cáp được sử dụng: STP, UTP, cáp quang, cáp đồng trục…
  - Kiểm tra kiến trúc và những ràng buộc về môi trường để chắc chắn những thành phần sau phải được thực hiện trong thiết kế:
    - Điều hòa không khí
    - Kiểm soát độ ẩm
    - Nguồn điện
    - Khóa cửa
    - Vv…

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.4 Kiểm tra khả năng hoạt động của mạng

- Cần thiết lập đường cơ sở cho mạng vì đường cơ sở mạng để xác định đặc tính của mạng trong điều kiện bình thường. Từ hiệu năng cơ sở, ta có thể xác định các vấn đề mạng.
- Đường cơ sở mạng xác định đặc tính của mạng dưới điều kiện bình thường.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.4 Kiểm tra khả năng hoạt động của mạng

- Để xây dựng được đường cơ sở ta cần đi phân tích các đặc tính sau của hệ thống mạng:
  - Phân tích tính sẵn sàng của mạng
  - Phân tích khả năng sử dụng của mạng
  - Phân tính độ chính xác của mạng (khả năng xảy ra lỗi)
  - Phân tích tính hiệu quả của mạng
  - Phân tích độ trễ và thời gian đáp ứng của mạng
  - Lập danh sách kiểm tra tình trạng hoạt động của mạng.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1.5 Phân tích luồng lưu thông dữ liệu trên mạng

- Xác định đặc tính luồng lưu thông dữ liệu
  - Đặc tính về luồng lưu thông bao gồm việc xác định địa chỉ nguồn, đích của lưu thông mạng, phân tích hướng và tính đối xứng của dữ liệu truyền giữa nguồn và đích.
  - Trong một vài ứng dụng thì luồng bao gồm cả hai chiều và đối xứng(cả hai đầu gửi thông tin ở cùng một tốc độ) hoặc bất đối xứng (client gửi một yêu cầu nhỏ, server trả về một lượng lớn dữ liệu), ứng dụng broadcast (quảng bá), luồng là một chiều và không đối xứng.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Đo lường, phân tích hành vi luồng lưu thông dữ liệu có thể giúp người thiết kế xác định loại router sẽ được sử dụng trong hệ thống. Đo lưu lượng mạng cũng giúp người thiết kế rõ hơn về yêu cầu của mạng thiết kế như:
  - Biết được đặc tính của hành vi mạng đang tồn tại
  - Kế hoạch phát triển và mở rộng mạng
  - Đánh giá hiệu năng mạng
  - Kiểm tra chất lượng của dịch vụ mạng

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Cách thức đo kích thước của một luồng là đo số megabyte trên một giây của truyền thông giữa các thực thể (MBps).
  - Có các loại luồng lưu thông của các ứng dụng sau:
    - Terminal/host traffic flow
    - Client/server traffic flow
    - Peer to peer traffic flow
    - Server/server traffic flow
    - Distributed computing traffic flow

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Để đo kích thước của luồng, sử dụng một bộ phân tích giao thức ghi lại tải giữa hệ thống nguồn, đích. Có thể sử dụng Cisco NetFlow để thu thập và đo dữ liệu được nhập vào trên interface của router hoặc switch, bao gồm địa chỉ IP nguồn, đích, TCP, UDP nguồn, đích, số gói tin và số byte. Lập bảng thống kê như dưới đây:

	Đích 1		Đích 2		Đích 3		Đích n	
	MBps	Path	MBps	Path	MBps	Path	MBps	Path
Nguồn 1								
Nguồn 2								
….	….		….		….		…..	
Nguồn n								

- Bảng trên bao gồm các thông tin về nguồn, đích, lượng lưu thông (MBps), để điền các thông tin ta cần đặt một thiết bị quản trị trong lớp core của mạng để tập hợp dữ liệu trong một hoặc hai ngày. Để có thông tin về đường đi, ta có thể xem các bản ghi về đường đi trong bảng định tuyến

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Lập tài liệu luồng lưu thông cho những ứng dụng mạng hiện có và ứng dụng mới
  - Để lập tài liệu cho luồng lưu thông cho ứng dụng mới (và ứng dụng hiện có), đặc tính từng loại luồng cho mỗi ứng dụng và danh sách nhóm người dùng và dữ liệu lưu trữ liên kết với các ứng dụng, thực hiện lập bảng sau:

Đặc tính luồng lưu lượng ứng dụng mạng						
Tên ứng dụng	Loại luồng lưu thông	Giao thức được sử dụng bởi ứng dụng	Nhóm người dùng sử dụng ứng dụng	Kho lưu trữ dữ liệu	Băng thông được yêu cầu bởi ứng dụng	Yêu cầu chất lượng dịch vụ

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Tính toán lượng lưu thông:
  - Để tính được lưu lượng ta cần chú ý tới các tham số:
    - Số máy trạm
    - Thời gian rỗi trung bình giữa các máy gửi frame
    - Thời gian yêu cầu truyền lại trong môi trường truy cập
  - Traffic load (lượng tải) là tổng tất cả dữ liệu trên tất cả các node mạng sẵn sàng gửi ở thời gian riêng biệt. Ta thường thiết kế mạng có dung lượng nhiều hơn so với lượng dữ liệu mà nó có thể truyền.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Ước tính lượng lưu thông dữ liệu của ứng dụng
  - Để ước lượng về băng thông yêu cầu của một ứng dụng, ta cần nghiên cứu kích thước của dữ liệu được gửi bởi ứng dụng, kích thước tiêu đề của giao thức, và bất kỳ các thông tin bổ sung.
  - Ta khó có thể đoán đúng kích thước trung bình của một đối tượng dữ liệu truyền từ một người dùng tới một server, tuy nhiên ta có thể biết về kích thước phần tiêu đề của một số giao thức phổ biến, từ đó ta có thể ước lượng chính xác hơn về kích thước của dữ liệu.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Để giảm lưu thông dữ liệu không cần thiết bằng cách chọn giao thức định tuyến
  - Ta có thể sử dụng các giao thức định tuyến như OSPF, EIGRP các giao thức sử dụng ít băng thông hơn, chỉ cập nhật những thông tin thay đổi.
  - Trong khi các giao thức cũ như RIP thì gửi thông tin cập nhật dạng quảng bá do vậy sẽ tốn lưu lượng truyền nhiều hơn

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- Một số đặc điểm cần chú ý khi phân tích thiết kế:
  - Broadcast/Multicast
    - Gói tin quảng bá sẽ được gửi tới tất cả các trạm trong một mạng LAN. Có dịa chỉ MAC là: FF:FF:FF:FF:FF:FF
    - Với multicast thì một frame chỉ gửi tới một nhóm các trạm, địa chỉ là: 01:00:0C:CC:CC:CC được gửi bởi router và switch Cisco chạy giao thức CDP
    - Ở lớp 2 thì các thiết bị như switch, bridge sẽ chuyển tiếp broadcast, multicast frame tới tất cả các port khác, ngoại trừ port nhận.
    - Ở lớp 3, router không chuyển tiếp broadcast, thế nên ta sử dụng router để chia ra thành các miền broadcast.
    - Ở lớp 2 ta cũng có thể sử dụng VLAN để chia LAN thành các miền broadcast

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2 Phân tích và xác định các yêu cầu an toàn

- Xác định và phân loại tài sản mạng
- Xác định mục tiêu, yêu cầu an toàn
- Xác định điểm yếu, lỗ hổng, hiểm họa
- Các giải pháp an toàn

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.1. Xác định và phân loại tài sản mạng

- Data: tệp tin, thư mục
- Phần mềm: HĐH, ứng dụng, dịch vụ
- Thiết bị đầu cuối: Server, PC
- Thiết bị mạng: Router, Switch, FW, IDS, AP
- Người dùng mạng

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.2. Phân tích các yêu cầu an toàn

Việc thiết kế mạng an toàn thì nó phải đáp ứng 3 yêu cầu cơ bản:

- Tính bí mật của dữ liệu
- Tính toàn vẹn của dữ liệu
- Tính sẵn sàng của dữ liệu và hệ thống

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.2. Phân tích các yêu cầu an toàn

- Khả năng kiểm soát truy cập của mạng
- Khả năng phát hiện và ngăn chặn tấn công
- Khả năng phòng chống mã độc
- Đảm bảo an toàn về mặt vật lý
- Sự hiểu biết của người dùng về ATTT
- Bản quyền phần mềm
- Đảm bảo ATTT trên kênh truyền

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Data: Tệp tin, thư mục

- Bị đọc trộm
- Thay đổi nội dung
- Xóa dữ liệu
- Sao chép bất hợp pháp

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Data: Tệp tin, thư mục

Giải pháp:

- Mã hóa
- Xác thực, phân quyền
- Sao lưu

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Phần mềm: HĐH, ứng dụng, dịch vụ

- Mật khẩu, Tường lửa, Tự động cập nhật bản vá,
- Phân quyền chưa chính xác
- Lỗ hổng phần mềm
- Truy cập bất hợp pháp
- Tấn công mạng
- Mã độc hại

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Phần mềm: HĐH, ứng dụng, dịch vụ

Giải pháp:

- Mật khẩu mạnh,
- Phân quyền chặt chẽ
- Kích hoạt FW, Update
- Công nghệ FW, IDS, SIEM
- Antivirus
- Đăng ký sở hữu trí tuệ

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Thiết bị đầu cuối: Server, PC

- Không có tủ Rack
- Hỏng ổ cứng
- Không có phòng máy chủ riêng
- Không có điều hòa,
- Không có thiết bị dự phòng điện
- Bị tấn công về mặt vật lý
- Bị tấn công truy cập

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Thiết bị đầu cuối: Server, PC

Giải pháp:

- Hệ thống phòng có khóa
- Hệ thống tủ Rack, điều hòa,
- Thiết bị dự phòng điện
- Hệ thống camera giám sát
- Xác thực vân tay
- RAID

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

Thiết bị mạng: Router, Switch, Firewall, AP

- Không có tủ Rack
- Không có phòng máy chủ riêng
- Không có điều hòa,
- Không có thiết bị dự phòng điện
- Bị tấn công về mặt vật lý
- Bị tấn công truy cập

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

User:

- Nhóm người dùng thường: Chưa được trang bị kiến thức về ATTT
- Nhóm quản trị: Kiến thức về ATTT còn yếu
- Bị tấn công bằng kỹ nghệ xã hội
- Vô ý thức trong quá trình sử dụng
- Cố ý tấn công mạng

CHƯƠNG 4. PHÂN TÍCH MẠNG THIẾT KẾ

4.2.3. Xác định điểm yếu, lỗ hổng, hiểm họa

User:

Giải pháp:

- Đào tạo nâng cao nhận thức
- Thiết lập chính sách AT quy định quyền hạn truy cập tài nguyên

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2.2 Quy trình đánh giá phân tích rủi ro

1. ***Xác định rủi ro***
2. ***Phân tích và ước lượng rủi ro***
3. ***Xử lý các rủi ro***

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

- **Quy trình đánh giá phân tích rủi ro**

1. ***Xác định rủi ro [1]:***
   a) Xác định tất cả các tài sản trong phạm vi hệ thống quản lý
   b) Xác định các điểm yếu có thể tồn tại trong tài sản
   c) Xác định các mối đe dọa đối với tài sản
   d) Xác định các tác động làm mất tính bí mật, toàn vẹn, sẵn sàng của tài sản.

[1] TCVN 27001:2009

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

2. Phân tích và ước lượng rủi ro

a) Đánh giá các ảnh hưởng tới hoạt động của tổ chức có thể gây ra do sự cố về ATTT.

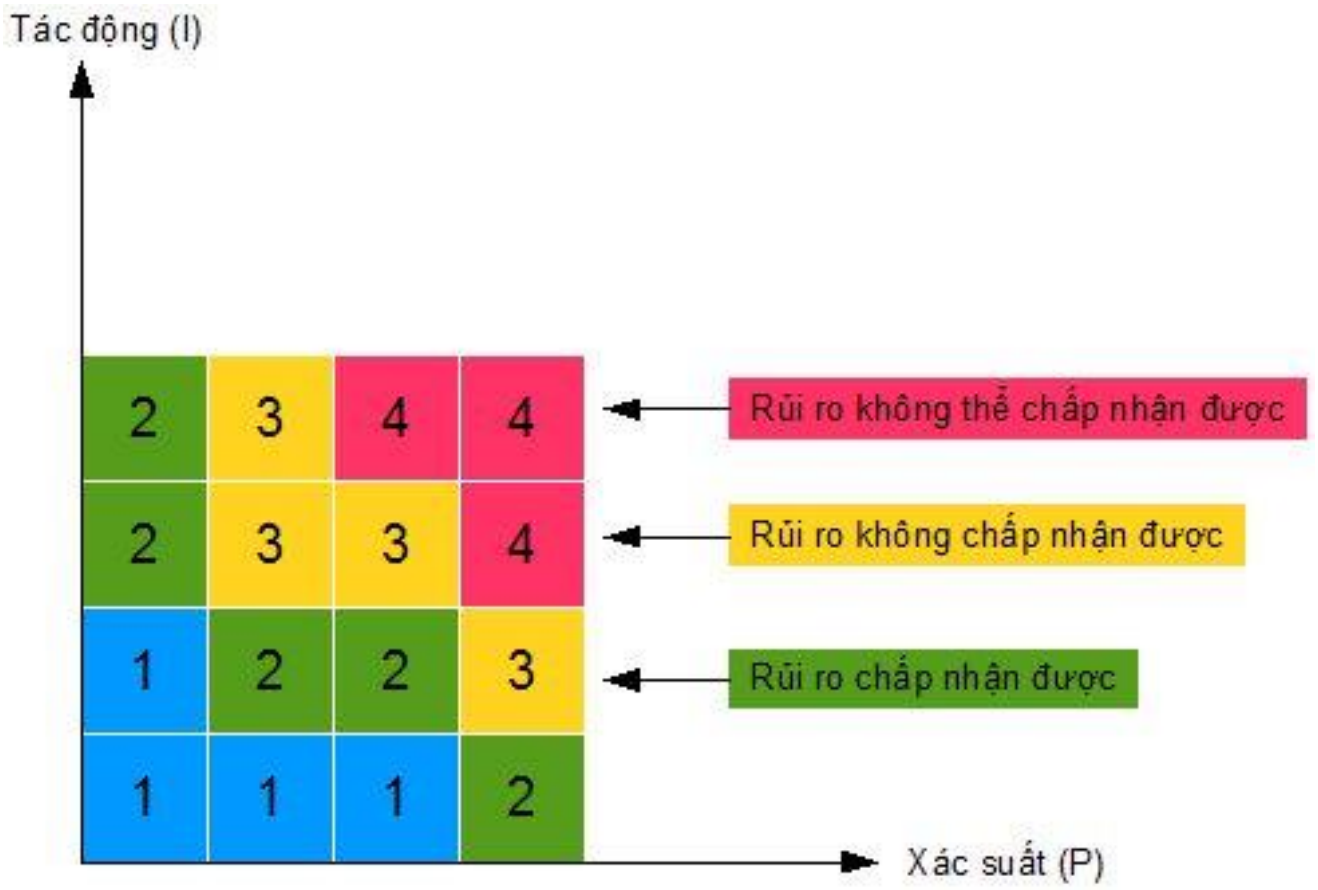
b) Đánh giá các khả năng thực tế có thể xảy ra sự cố ATTT bắt nguồn từ các mối đe dọa và điểm yếu đã dự đoán.

c) Ước đoán các mức độ của rủi ro.

d) Xác định rủi ro là chấp nhận được hay phải có biện pháp xử lý dựa trên các tiêu chí chấp nhận rủi ro đã thiết lập.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

Sơ đồ mức độ rủi ro:



CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3. Xử lý rủi ro

a) Chấp nhận rủi ro
b) Giảm thiểu rủi ro
c) Đẩy rủi ro sang nơi khác

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.1 Chấp nhận rủi ro

Tiêu chí chấp nhận rủi ro: Phụ thuộc vào chính sách, mục đích, mục tiêu của tổ chức và lợi ích của các bên liên quan.

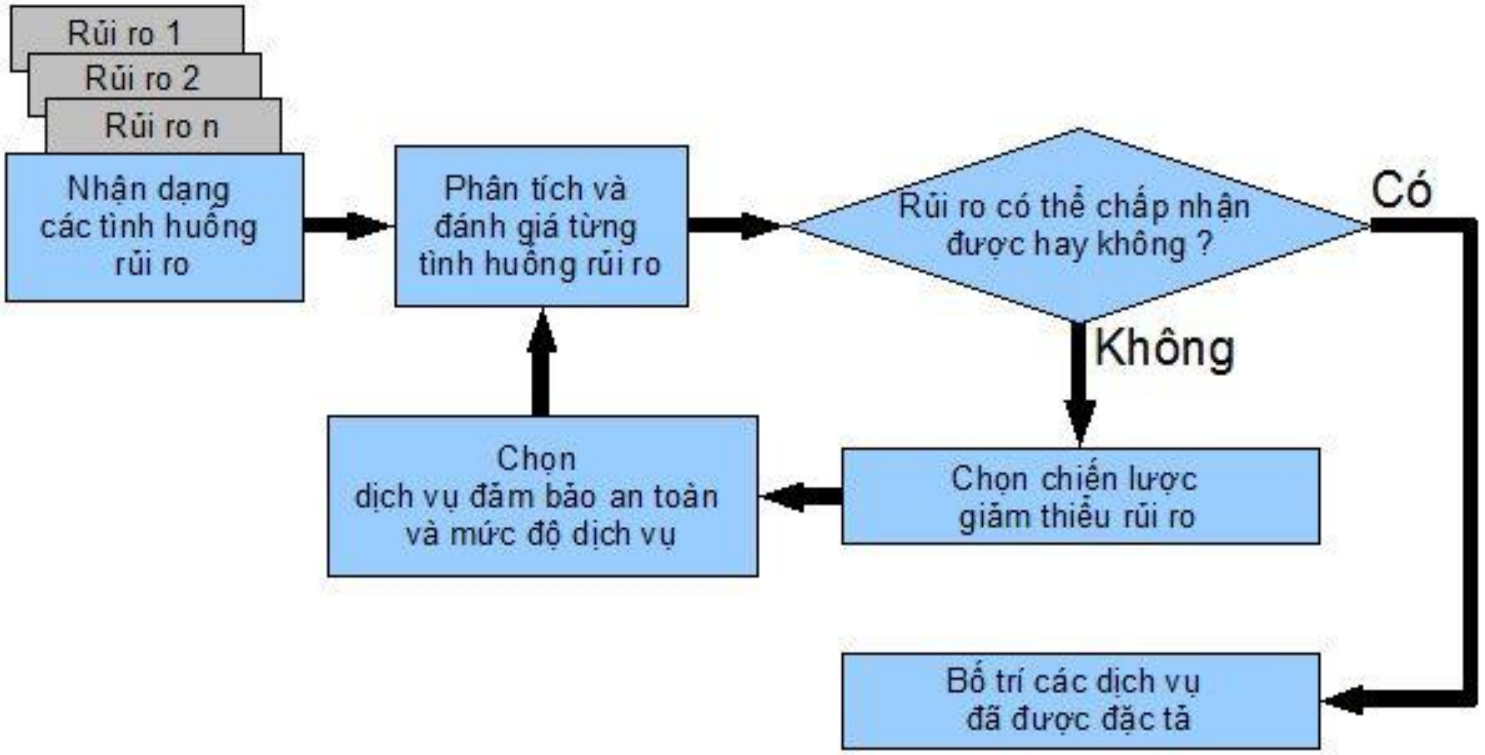
Vd: - rủi ro do lộ thông tin cổng dịch vụ

- rủi ro lộ thông tin về website và lĩnh vực hoạt động

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2 Giảm thiểu rủi ro

- Giảm thiểu trực tiếp: Là quyết định những biện pháp cần áp dụng cho mỗi kịch bản rủi ro.



CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2 Giảm thiểu rủi ro

- Giảm thiểu gián tiếp: Đưa ra các chính sách đảm bảo an toàn

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.3 Đẩy rủi ro sang nơi khác (dịch chuyển rủi ro)

- Dịch chuyển rủi ro thường liên quan đến việc lập hợp đồng phân định trách nhiệm liên đới giữa thực thể và các cơ quan, tổ chức trung gian
- Trường hợp điển hình của dịch chuyển rủi ro chính là hợp đồng bảo hiểm, và các ghi nhớ.

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2.3 Xác định các yêu cầu an toàn

- Việc thiết kế mạng an toàn thì nó phải đáp ứng được 3 yêu cầu đó là:
  - Tính bí mật của dữ liêu: chỉ những người dùng được quyền mới được xem những thông tin nhạy cảm.
  - Tính toàn vẹn của dữ liệu: chỉ những người dùng được quyền mới có thể thay đổi dữ liệu nhạy cảm.
  - Tính sẵn sàng: hệ thống và dữ liệu phải luôn sẵn sàng, vì thế người dùng không bị gián đoạn khi truy cập vào những tài nguyên.
- Phải đặt ra các chỉ tiêu cụ thể đối với từng yêu cầu trên

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2.3 Xác định các yêu cầu an toàn

- Ngoài ra các cơ chế đảm bảo an toàn còn phải đáp ứng các yêu cầu sau đây:
  - Cho phép người dùng bên ngoài (khách hàng, nhà cung cấp) truy cập dữ liệu trên web hay tập tin trên máy chủ FTP công khai hoặc các dịch vụ công khai khác, nhưng không được phép truy cập vào dữ liệu nội bộ
  - Thực hiện ủy quyền và xác thực đối với người dùng văn phòng tại các chi nhánh, người dùng điện thoại di động, người dùng làm việc từ xa

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2.3 Xác định các yêu cầu an toàn

- Phát hiện những kẻ xâm nhập trái phép và khoanh vùng được những thiệt hại do những kẻ xâm nhập trái phép gây ra
- Bảo vệ vật lý các thiết bị mạng, máy chủ, máy trạm vv.. (ví dụ, để các thiết bị trong các phòng được khóa).

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2.3 Xác định các yêu cầu an toàn

- Bảo vệ dữ liệu trên đường truyền giữa các chi nhánh với trụ sở chính, giữa các chi nhánh với nhau thông qua mạng riêng ảo VPN
- Bảo vệ logic các thiết bị mạng, máy chủ, máy trạm... với tài khoản người dùng và các quyền truy cập cho các thư mục và tập tin

CHƯƠNG 3. PHÂN TÍCH MẠNG THIẾT KẾ

3.2.3 Xác định các yêu cầu an toàn

- Bảo vệ các ứng dụng và dữ liệu, tránh bị nhiễm virus
- Đào tạo nâng cao kiến thức và kỹ năng cho người dùng và người quản lý mạng về các rủi ro mất an toàn đối với hệ thống mạng và cách thức hạn chế và phòng chống
- Thực hiện quyền tác giả hoặc sử dụng pháp luật để bảo vệ sản phẩm và bản quyền sở hữu trí tuệ
- Đáp ứng các yêu cầu và tuân thủ các đòi hỏi về pháp lý.

Tổng kết chương 3

Giai đoạn phân tích có những kết quả gì?

- Biết được mục tiêu hoạt động của hệ thống mạng
- Xác định được các yêu cầu về kỹ thuật mạng cần đáp ứng
- Giải pháp ứng phó các rủi ro, hiểm họa có thể xảy ra
- Xác định được các yêu cầu về an toàn mà hệ thống mạng cần phải đáp ứng.