

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH (TN) (CO3094)

ASSIGNMENT 2 REPORT

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

Giảng viên hướng dẫn: Lê Bảo Khánh
Nhóm lớp: CN02
Sinh viên thực hiện: Nguyễn Hữu Nhân – 2252562 (Nhóm trưởng)
Trần Võ Anh Kiệt – 2052064
Chu Tuấn Nghĩa – 2053263
Bùi Tiến Trường Sơn – 2052242

TP. Hồ Chí Minh, tháng 11/2024

Mục lục

1	Danh sách thành viên và phân chia công việc	2
2	Yêu cầu kiến trúc hệ thống	3
3	Thiết kế hệ thống mạng	4
4	Mô tả cụ thể cho thiết kế mạng	5
4.1	Sơ đồ địa chỉ IP :	7
4.1.1	Trụ sở chính	7
4.1.2	Chi nhánh	8
4.2	Các Host trong hệ thống mạng :	8
4.3	Các thiết bị mạng :	8
5	Tính toán throughput, bandwidth và các thông số an toàn cho Mạng máy tính	10
5.1	Trụ sở chính	10
5.2	Chi nhánh	10
6	Đánh giá hệ thống	12
6.1	Độ tin cậy	12
6.2	Dễ dàng nâng cấp	12
6.3	Phần mềm hỗ trợ	12
6.4	Tính an toàn vào bảo mật của hệ thống	12
6.5	Những hạn chế còn vướng mắc trong dự án	13
6.6	Định hướng tương lai	13
7	Mô phỏng phần mềm	14
8	Bài làm	15
9	Tham khảo	15



1 Danh sách thành viên và phân chia công việc

STT	Họ và tên	Mã số sinh viên	Công việc	Phần trăm
1	Nguyễn Hữu Nhân	2252562	Thiết kế hệ thống Mô phỏng hệ thống	100%
2	Trần Võ Anh Kiệt	2052064	Thiết kế hệ thống Latex	100%
3	Chu Tuấn Nghĩa	2012822	Thiết kế hệ thống Mô phỏng hệ thống	100%
4	Bùi Tiến Trường Sơn	2052242	Thiết kế hệ thống Latex	100%

2 Yêu cầu kiến trúc hệ thống

CCC (Computer & Construction Concept) được yêu cầu thiết kế mạng máy tính để triển khai tại Trụ sở chính (tại Thành phố Hồ Chí Minh) và hai Chi nhánh (tại Đà Nẵng và Hà Nội) của Ngân hàng BB đang được xây dựng. Các đặc điểm chính của việc sử dụng CNTT ở Công ty này như sau .

Trụ sở chính:

- Tòa nhà Trụ sở chính gồm 7 tầng, tầng 1 được trang bị 1 phòng IT và Cable Central Local (dùng patch panel thu dây) .
- Quy mô trung bình: 120 máy trạm, 5 máy chủ, 12 thiết bị mạng (hoặc có thể nhiều hơn với các thiết bị dành riêng cho bảo mật) .
- Sử dụng các công nghệ mới cho cơ sở hạ tầng mạng bao gồm kết nối có dây và không dây, cáp quang (GPON) và GigaEthernet 1GbE/10GbE. Mạng được tổ chức theo cấu trúc VLAN cho các phòng ban khác nhau .
- Mạng con Trụ sở chính kết nối với 2 mạng con Chi nhánh bằng 2 đường truyền riêng để kết nối WAN (có thể áp dụng SD-WAN, MPLS) và 2 xDSL để truy cập Internet với cơ chế cân bằng tải. Tất cả lưu lượng truy cập vào Internet đều đi qua mạng con Trụ sở chính .
- Để mua lại phần mềm, công ty sử dụng kết hợp phần mềm được cấp phép và nguồn mở, ứng dụng văn phòng, ứng dụng máy khách-máy chủ, đa phương tiện và cơ sở dữ liệu .
- Yêu cầu về bảo mật cao (ví dụ: tường lửa, IPS/IDS, phát hiện lừa đảo), tính sẵn sàng cao (HA), độ mạnh mẽ khi xảy ra sự cố, dễ nâng cấp hệ thống .
- Đề xuất cấu hình VPN cho site-to-site và cho nhân viên làm việc từ xa kết nối với mạng LAN Công ty .
- Đề xuất hệ thống camera giám sát cho Công ty .

Chi nhánh:

- Tòa nhà có 2 tầng, tầng 1 được trang bị 1 phòng IT và 1 phòng Cable Central Local.
- Chi nhánh BB quy mô nhỏ: 30 máy trạm, 3 máy chủ, 5 thiết bị mạng trở lên .

Triển khai : Việc triển khai kết nối giữa Trụ sở chính và các Chi nhánh thông qua các liên kết WAN, chúng ta có thể lựa chọn một trong các công nghệ như SD-WAN, MPLS,... sử dụng cho liên kết này tùy theo tính kinh tế của giải pháp . Phân tích ưu nhược điểm của giải pháp được chọn .

Thông số : Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80 % vào giờ cao điểm 9g-11g và 15g-16g) có thể dùng chung cho Trụ sở và Chi nhánh như sau:

- Servers dùng cho cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu,..... Tổng dung lượng tải xuống ước tính khoảng 1000 MB/ngày và ước tính tải lên là 2000 MB/ngày.
- Mỗi workstation dùng cho để duyệt Web, tải tài liệu và giao dịch với khách hàng,... Ước tính tổng tải xuống khoảng 500 MB/ngày và ước tính tải lên là 100 MB/ngày.
- Thiết bị kết nối WiFi của khách hàng truy cập để tải về khoảng 500 MB/ngày.
- Hệ thống Mạng máy tính của Ngân hàng BB Bank được dự toán cho mức độ phát triển 20% trong 5 năm (về số lượng người sử dụng, tải trọng mạng, mở rộng nhiều chi nhánh,...).

3 Thiết kế hệ thống mạng

Các yêu cầu về kiến trúc cần có cho hệ thống:

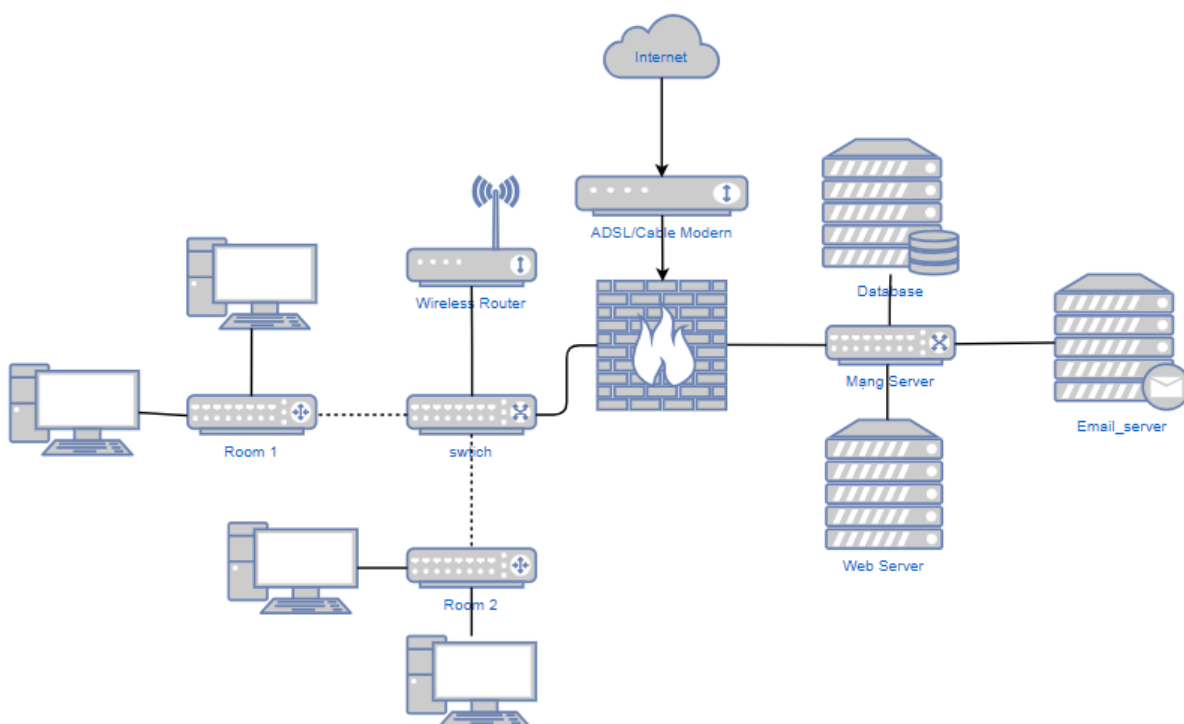
- Phân hệ kết nối internet: Phần này được trang bị các thiết bị kết nối Gateway Cisco Router riêng kết nối với mạng Internet, cho phép mở rộng và nâng cấp tốc độ cổng kết nối Internet tùy theo nhu cầu phát triển. Người dùng truy nhập vào mạng được xác thực tùy theo quyền truy nhập để vào mạng nội bộ hoặc Internet và CSDL dùng để xác thực được quản lý tập trung trên máy chủ ACS đặt ở vùng quản trị hệ thống .
- Phân hệ Server DMZ: Gồm hệ thống máy chủ Web, E-mail, máy chủ ứng dụng dành cho khách hàng, nội bộ truy nhập, trên máy chủ Web gồm có các hệ thống giao dịch trên WEB của Ngân hàng , Internet Banking , homeBanking, các thông tin quảng cáo, tra cứu các sản phẩm của ngân hàng. Ngoài ra còn các máy chủ CSDL lưu trữ các dữ liệu quan trọng của khách hàng, máy chủ này rất quan trọng đối với hệ thống ngân hàng vì nó chứa toàn bộ thông tin khách hàng, các thông tin giao dịch quan trọng của khách hàng, đảm bảo sự an toàn cho chúng mà một yêu cầu quan trọng cần đặt ra khi thiết kế hệ thống mạng này.
- Phân hệ mạng máy tính nội bộ : Gồm các workstations đặt tại các phòng ban của tòa nhà được sử dụng với nhu cầu công việc của các nhân viên của ngân hàng.
- Phân hệ Wireless LAN : Hỗ trợ các kết nối không dây có các thiết bị điện tử có thể kết nối không dây, hỗ trợ kết nối internet không dây cho nhân viên và khách hàng.
- Phân hệ kết nối với các chi nhánh khác của ngân hàng: Ngân hàng trung tâm kết nối với các chi nhánh của nó theo đường truyền riêng được thuê bởi bên thứ ba (ISP) kết nối với mạng WAN.
- Phân hệ bảo mật : Tường lửa

4 Mô tả cụ thể cho thiết kế mạng

Để kết nối các máy trạm và máy chủ tại trụ sở chính và chi nhánh ngân hàng, nhóm chúng em lựa chọn kiến trúc mạng hình sao (star topology) cho mạng LAN vì những ưu điểm sau:

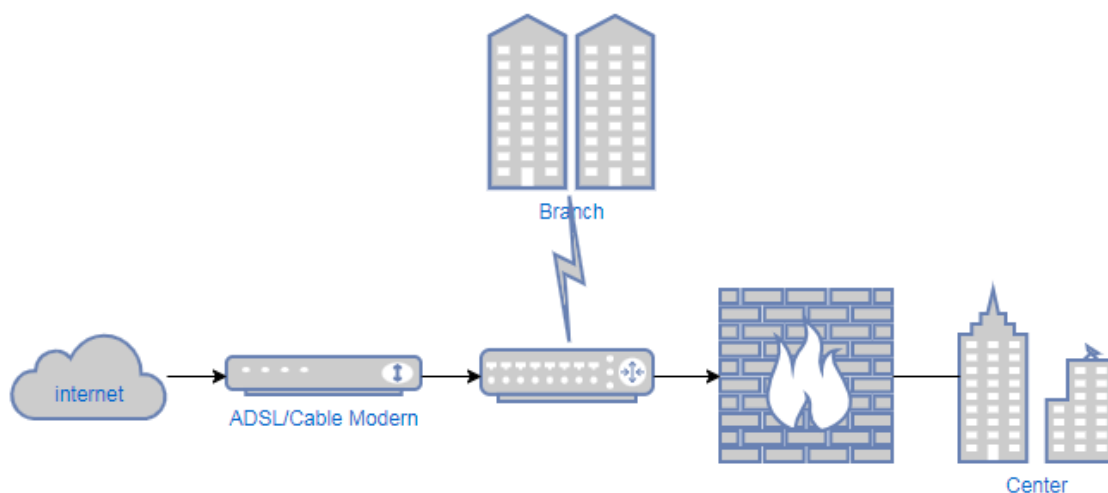
- Với kiến trúc sao, các thiết bị mạng nằm ở rìa hoạt động độc lập với nhau, do đó khi một thiết bị gặp sự cố thì các thiết bị khác vẫn hoạt động bình thường.
- Kiến trúc sao cho phép dễ dàng thêm mới các thiết bị mạng mà không làm ảnh hưởng nhiều tới hệ thống.
- Mô hình này phù hợp với mạng có tải nặng lớn như trong trường hợp của ngân hàng.

Mô hình logic của mạng LAN được minh họa chi tiết trong Hình 1. Toàn bộ mạng LAN nội bộ sẽ được kết nối đến tường lửa trước khi truy cập ra internet. Điều này nhằm mục đích bảo mật cho các máy chủ và thiết bị quan trọng bên trong ngân hàng.



Hình 1

- Trong thiết kế mạng cho hệ thống ngân hàng, việc kết nối Internet và liên kết WAN giữa các chi nhánh đóng vai trò rất quan trọng.
- Đối với kết nối Internet, mỗi địa điểm sẽ bố trí một thiết bị router kết nối tới modem ADSL nhằm cung cấp đường truyền Internet. Trên router áp dụng kỹ thuật NAT để ánh xạ địa chỉ IP nội bộ của mạng LAN sang địa chỉ IP public, giúp các thiết bị trong mạng LAN có thể truy cập Internet. NAT giúp tiết kiệm không gian địa chỉ IP public, đồng thời tăng tính bảo mật cho hệ thống.
- Đối với kết nối WAN, mỗi router được cấu hình thêm các đường truyền riêng kết nối tới các chi nhánh thông qua nhà cung cấp dịch vụ. Trên router áp dụng giao thức định tuyến OSPF để cân bằng tải, tăng hiệu suất sử dụng băng thông. Với thiết kế trên, mạng ngân hàng được kết nối Internet và WAN giữa các địa điểm một cách tin cậy, bảo mật và hiệu quả.

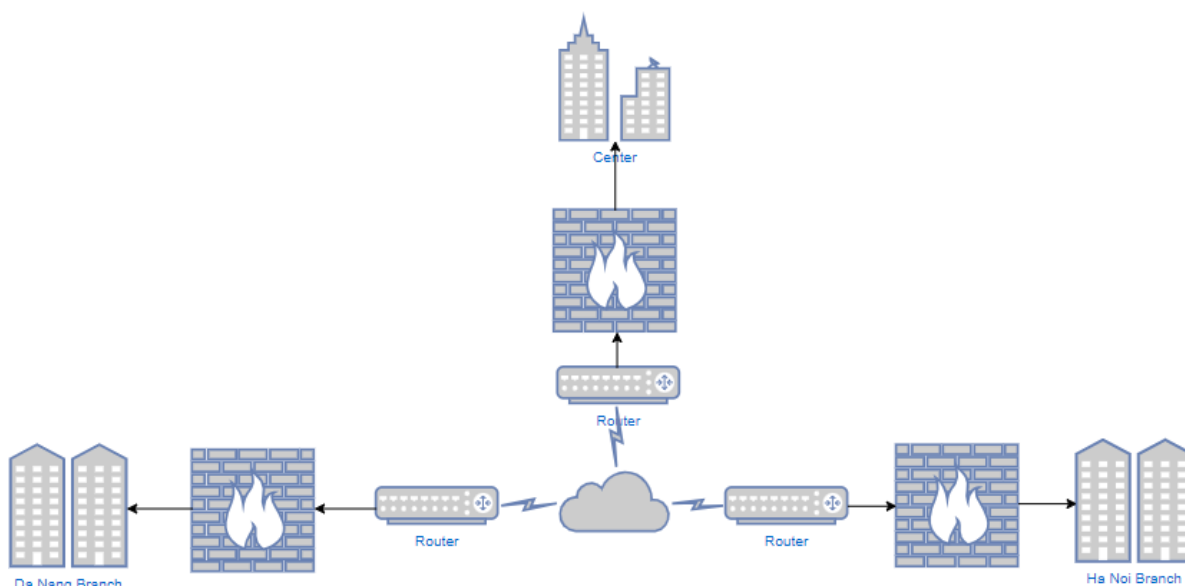


Hình 2

Để liên kết WAN giữa trụ sở chính và các chi nhánh, mỗi địa điểm sẽ được trang bị một thiết bị router kết nối đến các đường truyền riêng do nhà cung cấp dịch vụ cung cấp. Mỗi router sẽ được cấu hình 3 đường truyền WAN:

- Đường ADSL kết nối Internet
- Hai đường truyền riêng kết nối tới các chi nhánh khác

Trên router sẽ áp dụng giao thức định tuyến OSPF để cân bằng tải giữa các đường WAN. OSPF sẽ tự động tính toán và chọn đường đi tối ưu dựa trên thông số băng thông, tải của mỗi đường truyền. Giải pháp này giúp phân phối lưu lượng hiệu quả, tránh tắc nghẽn và nâng cao hiệu suất sử dụng băng thông.



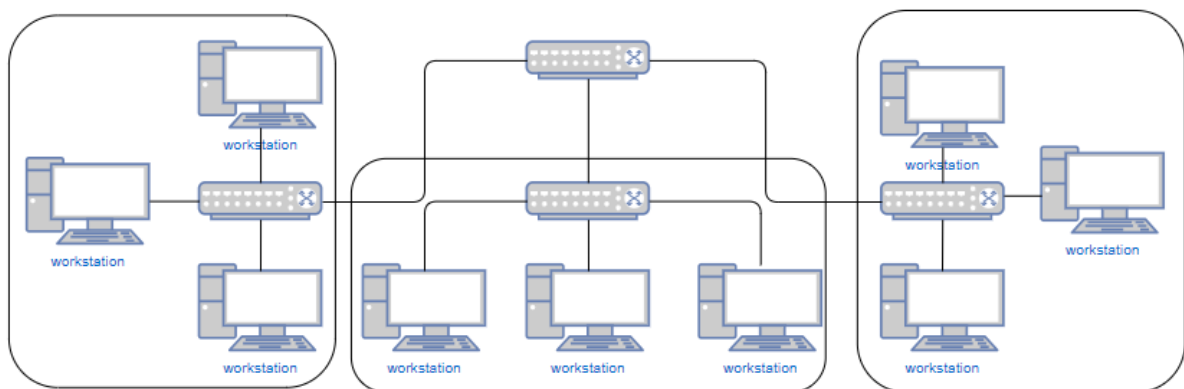
Hình 3

Để thiết kế mạng LAN cho các máy trạm và không dây tại mỗi địa điểm, chúng tôi lựa chọn kiến trúc hình sao vì các lý do sau:

- Các thiết bị ở rìa mạng hoạt động độc lập, tránh broadcast storm.
- Dễ dàng mở rộng thêm thiết bị mới mà không ảnh hưởng nhiều tới mạng.
- Các máy cùng bộ phận được nối chung switch và cùng VLAN để dễ dàng trao đổi thông tin.

Các switch tầng được tổng hợp lên một switch lõi layer 3 để liên kết xuống firewall và router. Sử dụng layer 3 switch để chuyển mạch giữa các VLAN khác nhau của các bộ phận. Mạng không dây được cung cấp bởi wireless router, kết nối tới layer 3 switch để tích hợp với mạng có dây.

Kiến trúc sao được áp dụng ở cả trụ sở chính và chi nhánh để đảm bảo tính nhất quán và dễ quản lý. Hình 3 minh họa cho cấu trúc mạng hình sao nhóm lựa chọn sử dụng, Hình 4 minh họa cho phần thiết kế này ở các chi nhánh.



Hình 4

4.1 Sơ đồ địa chỉ IP :

Bảng VLAN và phân vùng IP Private của trụ sở chính

4.1.1 Trụ sở chính

VLAN	Phòng ban	Địa chỉ mạng	Phân vùng IP Private	Tầng	workstations
10	Phòng kỹ thuật	192.168.10.0/24	192.168.10.1-192.168.10.255	Tầng 2	20
20	Lễ tân và CSKH	192.168.20.0/24	192.168.20.1-192.168.20.255	Tầng 1	20
30	Phòng Marketing	192.168.30.0/24	192.168.10.1-192.168.30.255	Tầng 3	20
40	Phòng Nhân Sự	192.168.40.0/24	192.168.10.1-192.168.40.255	Tầng 4	20
50	Phòng Tài Chính	192.168.50.0/24	192.168.10.1-192.168.50.255	Tầng 5	20
60	Phòng Quản Lý	192.168.60.0/24	192.168.10.1-192.168.60.255	Tầng 7	20
70	Wireless LAN	192.168.70.0/24	192.168.10.1-192.168.70.200	Tầng 1-7	No
	Server LAN	10.1.2.0/24	10.1.2.1-10.1.2.255	Tầng 6	No

Bảng 1: Bảng VLAN và phân vùng IP Private của trụ sở chính

4.1.2 Chi nhánh

VLAN	Phòng ban	Địa chỉ mạng	Phân vùng IP Private	Tầng	workstations
10	Phòng kĩ thuật	192.168.10.0/24	192.168.10.1-192.168.10.255	Tầng 2	5
20	Lễ tân và CSKH	192.168.20.0/24	192.168.20.1-192.168.20.255	Tầng 1	5
30	Phòng Marketing	192.168.30.0/24	192.168.10.1-192.168.30.255	Tầng 3	5
40	Phòng Nhân Sự	192.168.40.0/24	192.168.10.1-192.168.40.255	Tầng 4	5
50	Phòng Tài Chính	192.168.50.0/24	192.168.10.1-192.168.50.255	Tầng 5	5
60	Phòng Quản Lý	192.168.60.0/24	192.168.10.1-192.168.60.255	Tầng 7	5
70	Wireless LAN	192.168.70.0/24	192.168.10.1-192.168.70.200	Tầng 1-7	No
	Server LAN	10.1.2.0/24	10.1.2.1-10.1.2.255	Tầng 6	No

Bảng 2: Bảng VLAN và phân vùng IP Private của chi nhánh

4.2 Các Host trong hệ thống mạng :

1. Workstations: các máy tính văn phòng được cung cấp cho các nhân viên trong công ty sử dụng phục vụ nhu cầu trong công việc, gửi mail, sử dụng các ứng dụng văn phòng và các ứng dụng nội bộ của ngân hàng và các nhu cầu cơ bản khi sử dụng Internet.
2. Các máy khác kết nối mạng Wireless của ngân hàng như laptop, điện thoại thông minh của khách hàng hay nhân viên, liên kết sẽ cung cấp cung cấp một IP Private động cho các thiết bị kết nối và cung cấp liên kết Internet cho các thiết bị này.
3. Server: Các server cần thiết cho một hệ thống ngân hàng:
 - WebServer: Lưu trữ thông tin, xử lý các yêu cầu của khách hàng khi khách hàng sử dụng ứng dụng của ngân hàng.
 - Mail Server: Lưu trữ thông tin các email giao dịch .
 - Database server: Lưu trữ các thông tin khách hàng, thông tin giao dịch, thông tin nhân viên và các dữ liệu khác trong hệ thống ngân hàng. Đây cũng là bộ phận quan trọng của một ngân hàng vì nó chứa các thông tin các nhân quan trọng của khách hàng cần được đảm bảo an toàn trước những kẻ tấn công .
 - Với server có cùng một mục đích được thiết lập thêm để giảm thiểu sức nặng công việc trên 1 server chúng ta cần có cân bằng tải để điều hướng giữa hai Server này nhằm chia sẻ công việc trên mỗi Server và phản hồi yêu cầu kịp thời.

4.3 Các thiết bị mạng :

1. Firewall: Một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Chúng tôi lựa chọn tường lửa ASA 5506. Cisco ASA 5506 là một tường lửa đầy đủ tính năng cho các môi trường làm việc từ xa của doanh nghiệp và chi nhánh. Nó cung cấp tường lửa hiệu suất cao, SSL và IPsec VPN và các dịch vụ mạng phong phú trong một thiết bị hoạt động tức thì theo mô-đun. Sử dụng Trình quản lý thiết bị bảo mật thích ứng Cisco (ASDM) đồ họa tích hợp, Cisco ASA 5506 có thể được triển khai nhanh chóng và dễ dàng quản lý, giúp các doanh nghiệp giảm chi phí hoạt động. Nó có bộ chuyển mạch Gigabit Ethernet, các cổng có thể được nhóm động để tạo ra tối đa ba VLAN riêng biệt cho gia đình, doanh nghiệp và lưu lượng truy cập Internet để cải thiện phân đoạn mạng và bảo mật .
2. Switch :
 - Switch layer 2 2690-24TT : Đây là một thiết bị chuyển mạch của Cisco với 24 cổng FastEthernet 10/100 ports đây là cổng mà ta sẽ kết nối các host và kết nối với Switch tổng.

- Switch layer 3 3560 :24 cổng FastEthernet 10/100 ports, nhóm sử dụng chúng để kết nối với các Switch tại các node và 2 cổng Gigabit Ethernet để kết nối với tường lửa. Ngoài chức năng chuyển mạch Switch layer 3 còn có thể định tuyến nên khi kết nối các mạng con có nhiều Vlan khác nhau sử dụng Switch layer 3 mà một lựa chọn phù hợp, ngoài ra với yêu cầu chúng ta cũng có thể lựa chọn Router thay thế.

3. Router

- Wireless Router : Một thiết bị thực hiện các chức năng của bộ định tuyến và cũng bao gồm các chức năng của Access Point. Nó được sử dụng để cung cấp quyền truy cập vào Internet hoặc mạng máy tính riêng.
- Router PT: Thiết bị mạng có chức năng chuyển tiếp gói dữ liệu giữa các mạng máy tính. Ở hệ thống này chúng ta cần kết nối mạng cục bộ ngân hàng với mạng Internet, mạng WAN nên việc sử dụng Router là một yêu cầu bắt buộc. Chúng ta cần lựa chọn các Router có các cổng Gigabit Ethernet để kết nối với Modem, tường lửa và các cổng serial để kết nối với mạng WAN. Khi sử dụng Router, chúng ta cần cấu hình các giải thuật định tuyến và có cân bằng tải để tối ưu đường truyền, cải thiện tốc độ truyền mạng.

5 Tính toán throughput, bandwidth và các thông số an toàn cho Mạng máy tính

- Throughput - Thông lượng : thông lượng mạng đề cập đến lượng dữ liệu có thể được truyền từ nguồn đến đích trong một khung thời gian nhất định. Công suất thông lượng được đo bằng bit trên giây, nhưng nó cũng có thể được đo bằng dữ liệu trên giây .
- Bandwidth - Băng thông : Định nghĩa băng thông mạng có thể gây nhầm lẫn, nhưng về cơ bản, băng thông mạng được định nghĩa là dung lượng thông lượng truyền tối đa của mạng. Đó là thước đo lượng dữ liệu có thể được gửi và nhận tại một thời điểm. Băng thông được đo bằng bit, megabit hoặc gigabit trên giây. Khi mọi người sử dụng các chương trình hoặc phần mềm, họ muốn các yêu cầu của họ được lắng nghe và đáp ứng kịp thời. Các gói bị mất khi truyền dẫn đến hiệu suất mạng kém hoặc chậm và thông lượng thấp cho thấy các vấn đề như mất gói. Sử dụng thông lượng để đo tốc độ mạng rất tốt cho việc khắc phục sự cố vì nó có thể tìm ra nguyên nhân chính xác của mạng chậm và cảnh báo cho quản trị viên về các vấn đề cụ thể liên quan đến mất gói.
- Việc tính toán thông lượng và băng thông của mạng là cần thiết, bởi nó sẽ cho chúng ta biết thiết kế mạng đã đáp ứng được những yêu cầu dịch vụ mà hệ thống mạng cung cấp hay chưa và có thể điều chỉnh sao cho phù hợp. Các yêu cầu dịch vụ mà hệ thống cần đáp ứng như là:
 - Truy cập Internet lướt web, chạy các ứng dụng khác trên máy tính, điện thoại thông minh.
 - Nhận và hồi đáp yêu cầu Web Server từ bên ngoài, hoặc nội bộ trong ngân hàng.
 - Nhận yêu cầu dữ liệu từ các trụ sở khác của ngân hàng.
 - Gửi mail, các dịch vụ gửi tin nhắn khác.

5.1 Trụ sở chính

Các thông số về lưu lượng và tải của hệ thống tập trung khoảng 80% vào giờ cao điểm 9h-11h và 15g-16h (tổng 3 giờ).

- Lượng Upload và Download 3000 MB/ngày cho mỗi server. Ở trụ sở chính có 5 server, do đó tổng lượng Upload và Download là: $5 * 3000 = 15000$ (MB)
- Với mỗi Workstation có tổng dung lượng Upload và Download khoảng 600 MB/ngày . Ở trụ sở chính có 120 Workstations , tổng dung lượng cần đáp ứng cho các Workstations: $120 * 600 = 72000$ (MB). Với mạng không dây, thiết bị kết nối WiFi của khách hàng truy cập để tải về khoảng 500 MB/ngày . Với trụ sở : trụ sở có khoảng 240 thiết bị mạng truy cập mỗi ngày . Tổng dung lượng cho wireless : $500 * 240 = 120000$ (MB).

Tại các giờ cao điểm, đường truyền mạng hoạt động hết công suất, và thông lượng tại các thời điểm này có giá trị cao nhất và đây cũng là giá trị gần với băng thông của mạng nhất, lưu lượng qua mạng tại những thời điểm này chiếm 80% toàn bộ dung lượng qua mạng trong ngày.

- Bandwith : $(15000 + 72000 + 120000) * 0.8 / (3 * 3600) = 15.3333$ (Mb/s)
- Thourghput : $(15000 + 72000 + 120000) * 0.8 / (24 * 3600) = 1.9167$ (Mb/s)

5.2 Chi nhánh

Các thông số về lưu lượng và tải của hệ thống tập trung khoảng 80% vào giờ cao điểm 9h-11h và 15g-16h. (3 giờ).

- Tổng Lượng upload và download 3000MB/ngày cho mỗi Server. Ở trụ sở chi nhánh chúng ta có 3 Server, tổng dung lượng upload và download : $3 * 3000 = 9000$ (MB) .

- Với mỗi Workstations có tổng dung lượng upload và download khoảng 600MB/ngày. Chúng ta có 30 Workstations: tổng dung lượng cần đáp ứng cho các Workstations: $30 * 600 = 18000$ (MB/ngày). Với mạng không dây, thiết bị kết nối WiFi của khách hàng truy cập để tải về khoảng 500 MB/ngày. Với trụ sở trụ sở có khoảng 150 thiết bị mạng truy cập mỗi ngày. Tổng dung lượng cho mạng Wireless: $150 * 500 = 75000$ (MB/ngày).

Tại các giờ cao điểm, đường truyền mạng hoạt động hết công suất, và thông lượng tại các thời điểm này có giá trị cao nhất và đây cũng là giá trị gần với băng thông của mạng nhất, lưu lượng qua mạng tại những thời điểm này chiếm 80% toàn bộ dung lượng qua mạng trong ngày.

- Bandwith : $(9000 + 18000 + 75000) * 0.8 / (3 * 3600) = 7.555$ (Mb/s)
- Thourghput : $(9000 + 18000 + 75000) * 0.8 / (24 * 3600) = 0.9444$ (Mb/s)

6 Đánh giá hệ thống

6.1 Độ tin cậy

Hệ thống có thể đáp ứng các yêu cầu về lưu lượng dữ liệu mà hệ thống cần đáp ứng. Các thiết bị trong mạng LAN có thể kết nối, giao tiếp với nhau trong mạng cục bộ.

6.2 Dễ dàng nâng cấp

Trong thời kì công nghệ không ngừng phát triển, hệ thống mạng được thiết kế cần đảm bảo có thể nâng cấp khi cần thiết. Chẳng hạn như tăng nhân sự, tăng chi nhánh hay tăng số lượng Server khi lượng khách hàng và nhu cầu của họ tăng lên. Hiện tại với nhu cầu 100 workstations tại trụ sở chính, nhóm đang sử dụng 6 switch với 24 port cho mỗi switch có thể đáp ứng cho 138 host, nên với nhu cầu tăng nhân viên hệ thống hiện tại vẫn đáp ứng được. Nếu trong trường hợp các Switch hiện tại không thể đáp ứng được nữa, chúng ta chỉ cần thêm Switch để kết nối các workstations mới và nối nó vào Switch layer 3 trung tâm. Với nhu cầu tăng Server, nếu Server cần tăng để phục vụ nhu cầu mới của hệ thống thì chúng ta chỉ cần kết nối các Server mới và Switch trung tâm tại mạng server và thiết lập địa chỉ private và ánh xạ địa chỉ public tĩnh cho nó. Nhưng nếu chúng ta cần thêm Server với mục đích giảm gánh nặng công việc cho một Server đang có sẵn trong hệ thống do Server hiện tại không còn đáp ứng đủ yêu cầu, thì thực hiện việc thêm này sẽ vất vả hơn so với nhu cầu thêm đặt ra ở trước vì chúng ta cần kết nối các Server có dùng chức năng vào cùng một Switch và sử dụng cân bằng tải để phân chia tải xuống các Server, đảm bảo các Server làm việc đồng đều.

6.3 Phần mềm hỗ trợ

Sử dụng các thiết bị mạng của Cisco- công ty hàng đầu về thiết bị mạng, chúng ta được sử dụng các thiết bị ổn định với kỹ thuật tốt các có tích hợp các phần mềm công nghệ mới nhất tối ưu nhất, phù hợp với yêu cầu sử dụng và cũng như có nhiều sự lựa chọn khi nâng cấp thiết bị mới.

6.4 Tính an toàn vào bảo mật của hệ thống

1. Yêu cầu mà hệ thống cần đáp ứng: đối với hệ thống ngân hàng, hệ thống hoạt động với nhu cầu xử lý thông tin dữ liệu nghiệp vụ quan trọng. Nhưng yêu cầu bảo mật mà hệ thống cần đáp ứng: Không cho phép đối tượng bên ngoài truy cập và nhưng hoạt động nghiệp vụ cũng như dữ liệu trong hệ thống, kiểm soát truy cập của người sử dụng, đảm bảo dữ liệu vào và ra an toàn.
2. Các tài nguyên cần bảo vệ trong hệ thống: Phần hệ Server là một phần quan trọng của hệ thống và cần được bảo vệ an toàn vì nó chứa những dữ liệu quan trọng của khách hàng cũng như các thông tin giao dịch cần được bảo mật. Khi phần hệ này bị tấn công với mục đích xấu nó có thể ảnh hưởng nghiêm trọng đến khách hàng của ngân hàng và các hoạt động của ngân hàng.
3. Những mối đe dọa mà hệ thống có thể gặp phải: Hacker sử dụng các công cụ, phần mềm mã độc tấn công hệ thống lấy cắp thông tin khách hàng, kiểm soát các máy tính trong ngân hàng. Ngoài những nguy cơ tìm ẩn ở bên ngoài, những người sử dụng các thiết bị trong mạng LAN cũng là một mối đe dọa lớn khi họ có ý định tấn công hệ thống, đây là một nguy cơ có thể gây ra thiệt hại rất lớn cho ngân hàng bởi nó rất khó để kiểm soát.
4. Các biện pháp khắc phục: Sử dụng tường lửa kiểm soát các gói tin được phép vào và ra khỏi hệ thống, mạng LAN các workstations và mạng Server được kết nối tường lửa theo hai đường khác nhau, nó góp phần kiểm soát các yêu cầu mà nhân viên trong hệ thống gửi đến cho Server. Sử dụng tường lửa phần nào ngăn chặn nhưng mối nguy cơ bên ngoài và bên trong của hệ thống. Ngoài ra với hệ điều hành và những ứng dụng mà hệ thống sử dụng cũng cần được sao lưu, bảo trì cập nhật thường xuyên để phát hiện ra các lỗi, lỗ hổng cũng như nâng cấp phần mềm công nghệ trong hệ thống, tiếp cận với những công nghệ với an toàn hơn tối ưu hơn. Bảo trì hệ thống thường xuyên cùng mà một giải pháp tốt cho vấn đề này và đây cũng là một yêu cầu bắt buộc đối với một hệ thống ngân hàng, bảo trì hệ thống thường xuyên giúp kịp thời phát hiện các lỗ hổng về bảo mật, cập nhật, thay mới các phần mềm cũng như phần cứng, an toàn hơn, hiện đại hơn, tối ưu hơn,...Bảo mật các thiết bị mạng trong hệ thống .

5. Các yêu cầu khi gặp sự cố: Cần ngắt toàn bộ kết nối Internet của hệ thống để chặn các kết nối trái phép ở bên ngoài, sử dụng backup Server để sao lưu dữ liệu trong các Server, việc sao lưu cần được tiến hành thường xuyên, có phòng ban riêng quản lý, giám sát hệ thống mạng xử lý sự cố kịp thời. Ngoài ra cần xây dựng các biện pháp dự phòng, sẵn sàng đối mặt với rủi ro nếu chúng xảy ra.

6.5 Những hạn chế còn vướng mắc trong dự án

Những vấn đề về bảo mật luôn là những những nguy cơ tiềm ẩn đối với các hệ thống ngân hàng, chúng có thể mang lại những hậu quả vô cùng lớn khi hệ thống bị tấn công, mặc dù các hệ thống ngân hàng đã có các biện pháp bảo mật nhưng các vụ tấn công vẫn xảy ra mỗi năm, nên vấn đề xây dựng hệ thống bảo mật sao cho tối ưu nhất an toàn nhất vẫn là một vướng mắc của dự án. Có rất nhiều các thiết bị mạng trên thị trường với nhiều kỹ thuật và công nghệ mới, khi thiết kế một hệ thống mạng máy tính việc lựa chọn các thiết bị mạng sao cho phù hợp cũng là một công việc khó khăn bởi không chỉ yêu cầu về đáp ứng lưu lượng dữ liệu mà còn những yêu cầu về giá cả, công nghệ bảo mật, hiệu năng cũng cần được xem xét kỹ càng.

6.6 Định hướng tương lai

Cải thiện khả năng bảo mật của hệ thống mà một công việc cần nhiều thời gian, công sức, cần cải thiện liên tục nên đây là một công việc mà chúng ta cần chú trọng trong tương lai. Thay mới các thiết bị mạng, kịp thời cập nhật các phần mềm công nghệ mới. Nâng cấp và bảo trì hệ thống cũng là những nhiệm vụ không chỉ của hiện tại mà cần chú trọng hơn ở tương lai.

7 Mô phỏng phần mềm

Sử dụng phần mềm mô phỏng Packet Tracer (Cisco) , các bước thực hiện:

1. Lựa chọn các thiết bị mạng cần sử dụng.
2. Thiết kế sơ đồ mạng LAN của trụ sở và chi nhánh.
3. Liên kết các trụ sở và chi nhánh trong qua mạng WAN với Leased line.
4. Kết nối mạng LAN tại trụ sở và chi nhánh ra Internet qua Modem theo đường truyền mà nhà cung cấp dịch vụ Internet Cấu hình các thiết bị mạng, cấu hình địa chỉ IP private static cho các Workstations, accept chúng vào các VLAN tương ứng.
5. Thiết lập DHCP server tại Wireless Router để cung cấp IP private động cho các thiết bị truy cập mạng không dây
6. Cấu hình tường lửa xác định các gói tin được phép đi qua.
7. Sử dụng cơ chế NAT tại Router để ánh xạ các địa chỉ IP private sang địa chỉ IP public để các host có thể liên kết đến Internet.
8. Định tuyến tại các Router.
9. Kiểm tra bằng các lệnh ping,...

8 Bài làm

<https://github.com/BenNguyen1412/ASS2-MMT>

9 Tham khảo

<https://www.cisco.com/>

<https://vnexperts.vn/cau-hinh-nat-tren-router-cisco.html>

<https://vienthongxanh.vn/mang-hinh-sao-star-topology-cau-truc-uu-diem-va-han-che/>

<https://khs247.com/cau-truc-mang/>

<https://content.cisco.com/>

<https://www.congnghvienthong.com/tin-tuc/tim-hieu-ve-mang-may-tinh.html>

<https://www.thegioididong.com/game-app/may-tram-workstation-la-gi-dac-diem-va-cach-phan-biet-voi->