CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

THIẾT KẾ THI CÔNG

DỰ ÁN:

Đầu tư trang thiết bị đảm bảo an toàn thông tin tại Trung tâm dữ liệu tại Tổng cục Khí tượng thủy văn

ĐƠN VỊ TƯ VẤN **CHỦ ĐẦU TƯ**

Tháng 9 năm 2023

DANH MỤC BẢNG

DANH MỤC HÌNH

CÁC TỪ VIẾT TẮT VÀ CÁC KHÁI NIỆM

STT	Từ viết tắt	Khái niệm, giải thích từ ngữ
1	KTTV	Khí tượng thủy văn
2	CNTT	Công nghệ thông tin
3	BTNMT	Bộ tài nguyên & Môi trường
4	TCKTTV	Tổng cục Khí tượng thủy văn

1. THÔNG TIN CHUNG

1.1. Tên dự án

Tên dự án: **Đầu tư trang thiết bị đảm bảo an toàn thông tin tại Trung tâm dữ liệu tại Tổng cục Khí tượng thủy văn**

1.2. Chủ đầu tư, địa điểm đầu tư

Chủ đầu tư: Trung tâm dữ liệu – Tổng cục khí tượng thủy văn – Bộ tài nguyên và Môi trường;

Địa điểm đầu tư:

- Tổng cục Khí tượng Thủy văn – Bộ tài nguyên và Môi trường

- Địa chỉ: Số 8 Pháo Đài Láng, phường Láng Thượng, quận Đống Đa, Hà Nội

1.3. Đơn vị tư vấn

1.4. Các căn cứ pháp lý

Căn cứ Luật Đầu tư công ngày 27 tháng 6 năm 2019;

Căn cứ Nghị định số 68/2022/NĐ-CP ngày 22 tháng 9 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài nguyên và Môi trường;

Căn cứ Nghị định số 40/2020/NĐ-CP ngày 06 tháng 4 năm 2020 của Chính phủ quy định chi tiết thi hành một số điều của Luật Đầu tư công;

Căn cứ Nghị định số 73/2019/NĐ-CP ngày 05 tháng 9 năm 2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;

Căn cứ Quyết định số 1103/QĐ-BTNMT ngày 02 tháng 6 năm 2021 của Bộ trưởng Bộ Tài nguyên và Môi trường về việc phê duyệt chủ trương đầu tư dự án "Xây dựng hoàn thiện cơ sở dữ liệu tài nguyên môi trường kết nối liên thông với các cơ sở dữ liệu/hệ thống thông tin";

Căn cứ Quyết định số 3067/QĐ-BTNMT ngày 11 tháng 11 năm 2022 của Bộ trưởng Bộ Tài nguyên và Môi trường về việc phê duyệt điều chỉnh chủ trương đầu tư dự án "Xây dựng hoàn thiện cơ sở dữ liệu tài nguyên môi trường kết nối liên thông với các cơ sở dữ liệu/hệ thống thông tin";

Căn cứ Quyết định số 1024/QĐ-BTNMT ngày 25 tháng 4 năm 2023 của Bộ trưởng Bộ Tài nguyên và Môi trường về việc phê duyệt điều chỉnh chủ trương đầu tư dự án "Xây dựng, hoàn thiện Hệ thống thông tin, cơ sở dữ liệu tài nguyên môi trường (Giai đoạn I)";

Căn cứ Quyết định số 1876/QĐ-BTNMT ngày 30 tháng 9 năm 2021 của Bộ trưởng Bộ Tài nguyên và Môi trường về việc giao kế hoạch đầu tư công trung hạn vốn ngân sách nhà nước giai đoạn 2021-2025;

Căn cứ Công văn số 6508/BTNMT-KHTC ngày 31 tháng 10 năm 2022 của Bộ Tài nguyên và Môi trường về việc điều chỉnh kế hoạch đầu tư công trung hạn giai đoạn 2021-2025;

1.5. Qui mô dự án

Đầu tư mua sắm trang thiết bị đảm bảo an toàn thông tin tại Trung tâm dữ liệu tại Tổng cục Khí tượng thủy văn – Bộ tài nguyên & Môi trường đảm bảo các yêu cầu an toàn thông tin của Tổng cục Khí tượng thủy văn nói riêng và Bộ tài nguyên & Môi trường nói chung

2. TPHÂN TÍCH, LỰA CHỌN PHƯƠNG ÁN, GIẢI PHÁP KỸ THUẬT, CÔNG NGHỆ, THIẾT BỊ ĐƯỢC LỰA CHỌN.

2.1. Phân tích lựa chọn giải pháp đầu tư thiết bị, thuê thiết bị.

Để lựa chọn được phương án đầu tư hiệu quả, tiết kiệm, tránh chồng chéo lãng phí và có tính mở rộng trong tương lai, cần phân tích 2 phương án sau đây để lựa chọn phương án kỹ thuật, công nghệ cho việc nâng cấp Trung tâm dữ liệu của Tổng cục khí tượng thủy văn.:

- Phương án đầu tư thiết bị hạ tầng.

- Phương án thuê thiết bị hạ tầng trên nền tảng điện toán đám mây (Cloud).

Với tiêu chí đầu tư hạ tầng của dự án là đảm bảo hiệu năng, an toàn bảo mật cũng như khả năng tích hợp, mở rộng sau này của hệ thống, do đó việc lựa chọn giải pháp đầu tư trang bị hạ tầng phần cứng cần được cân nhắc, tính toán dựa trên tính cấp thiết của nghiệp vụ, yêu cầu về quy mô và mức độ đáp ứng của hệ thống cũng như khả năng cân đối vốn.

Dự án được triển khai trong năm 2023, giải pháp đầu tư nâng cấp hạ tầng trong phạm vi dự án này cần chọn phương án phù hợp với tiến độ triển khai dự án, nhanh chóng đưa hệ thống vào vận hành và phù hợp với điều kiện thực tế tại đơn vị, đảm bảo hiệu quả về tài chính.

Bảng sau đây so sánh ưu điểm và nhược điểm của phương án mua thiết bị và phương án thuê thiết bị hạ tầng Cloud:

Bảng 1. So sánh ưu điểm và nhược điểm của phương án mua thiết bị và phương

án thuê thiết bị hạ tầng Cloud

Tính năng	Hạ tầng vật lý	Hạ tầng cloud
Cách thức hoạt động	Là một máy chủ, thiết bị lưu trữ vật lý	Lưu trữ và hoạt động trên hệ thống hạ tầng Cloud (điện toán đám mây)
Độ ổn định	Hoàn toàn chủ động trong quản trị và vận hành hệ thống	Công nghệ Cloud giúp hệ thống hoạt động ổn định, khả năng uptime 99.99%
Tính sẵn sàng	- Tất cả data sẽ được lưu trữ trên thiết bị vật lý - Chỉ cần 1 HDD bị hỏng có thể toàn bộ data của bạn sẽ mất - Việc triển khai backup tốn nhiều chi phí	- Data lưu trữ tập trung trên hệ thống SAN không lưu trên thiết bị vật lý - Data được backup đều đặn - Nếu có 1 Server vật lý bị lỗi, Cloud Server của bạn vẫn hoạt động ổn định
Khả năng mở rộng	- Phải mua thiết bị phần cứng chuyên dụng khi nâng cấp - Thời gian downtime khi cần nâng cấp khá lâu	- Có thể mở rộng hoặc thu hẹp ngay lập tức khi có yêu cầu - Có thể mở rộng và thu hẹp nguồn tài nguyên không giới hạn dung lượng
Chi phí	Chi phí đầu tư một lần cho toàn bộ phần cứng, vận hành, bảo trì hệ thống cũng như triển khai backup (sao lưu)	Chi phí phải trả hàng năm cho nhu cầu thực tế sử dụng (CPU, RAM, HDD…được cấu hình theo yêu cầu)
Cấu hình lại Server	Phải mua thêm các thiết bị như RAM, HDD trong trường hợp nâng cấp	Có thể thiết lập lại cấu hình cho server 1 cách dễ dàng trong khoảng thời gian ngắn
Tính đồng bộ và tương thích	Có thể lựa chọn thiết bị đồng bộ, tương thích để kết nối với các thiết bị liên quan	Không đảm bảo tính đồng bộ, khó tương thích để kết nối với các thiết bị liên quan

Dự án đã đề ra tiêu chí đầu tư phải phù hợp với hạ tầng CNTT của TTDL, tương thích với các trang thiết bị kết nối được đầu tư ở giai đoạn trước đây của dự án. Hiện nay tại Trung tâm dữ liệu đang vận hành các máy chủ và thiết bị lưu trữ được mua sắm từ giai đoạn trước đây. Qua quá trình khảo sát hiện trạng, nhận thấy hệ thống thiết bị hoạt động ổn định, đảm bảo hiệu năng theo thiết kế và an toàn dữ liệu, không có sự cố nghiêm trọng.

Để đảm bảo tính nhất quán về nền tảng công nghệ và kế thừa từ giai đoạn trước, chúng tôi đề xuất tiếp tục lựa chọn hạ tầng vật lý như hiện nay sẽ đảm bảo tối ưu hóa về chi phí đầu tư và đạt hiệu quả cao trong vận hành, sử dụng, bảo trì hệ thống về sau.

Vì vậy áp dụng phương án đầu tư mua sắm máy chủ và thiết bị lưu trữ để nâng cấp và cài đặt vận hành tại Trung tâm dữ liệu sẽ phù hợp với mục tiêu và các tiêu chí kỹ thuật đã đề ra trong dự án này.

2.2. Phân tích lựa chọn Hệ thống máy chủ ứng dụng

a. Máy chủ đơn lẻ dạng rack (rack-mount server)

Hạng mục	Thuyết minh
Tình hình sử dụng hiện nay	Từ khi hệ thống Server được phát triển và được sử dụng rộng rãi trên toàn thế giới trong các phòng máy chủ, các TTDL… máy chủ dạng rack-mount (1U, 2U, 3U,…) được sử dụng rất phổ biến. Cùng với sự phát triển của CNTT và sự phát triển nhanh chóng của hệ thống các ứng dụng, nghiệp vụ, dòng máy chủ dạng rack-mount vẫn hoàn toàn có khả năng đáp ứng được nhu cầu đưa ra, tuy nhiên cùng với sự phát triển về chiều dọc lẫn chiều ngang của các cơ quan, các tổ chức, việc triển khai hệ thống CNTT sẽ gặp một số khó khăn nhất định về thời gian, tổ chức, quy hoạch, tiêu thụ điện năng...

Ưu điểm	Với các ứng dụng có quy mô vừa và nhỏ, nhu cầu mở rộng không lớn thì máy chủ đơn lẻ dạng rack-mount cho phép mang lại nhiều lợi ích như: - Kích thước máy chủ nhỏ gọn, linh hoạt trong việc lắp đặt và triển khai. - Công nghệ thiết kế mang lại khả năng mở rộng thuận tiện với nhiều loại cấu hình từ 01- 04 vi xử lý, hỗ trợ đầy đủ các khe mở rộng PCI thế hệ mới. - Thuận tiện trong cấu hình và quản trị từng thiết bị thông qua khả năng quản trị từ xa được tích hợp sẵn. - Phù hợp với các ứng dụng quản trị hệ thống, giám sát theo dõi nhờ khả năng tách biệt hoàn toàn về mặt vật lý giữa các đơn thể thiết bị với nhau. Đặc tính này của các máy chủ đơn lẻ cho phép khả năng cấu hình và áp dụng chính sách bảo mật được chi tiết và chặt chẽ hơn
Nhược điểm	Với một hệ thống cần sự mở rộng và tăng cường năng lực xử lý trong tương lai, các máy chủ dạng Rack mount sẽ tồn tại một số nhược điểm: - Không linh hoạt: khi số lượng máy chủ tăng lớn sẽ gây hạn chế bởi các dây kết nối máy chủ (dây mạng, dây nguồn...) - Hạn chế trong khả năng phối hợp vận hành: Các yêu cầu thay đổi trong trung tâm dữ liệu, yêu cầu nhiều người tham gia (Quản trị mạng, quản trị hệ thống, cán bộ khai thác…) - Tiêu tốn tài nguyên phục vụ hệ thống thiết bị máy chủ: Yêu cầu nguồn điện, hệ thống làm mát, không gian, con người và chi phí - Quản lý không đồng nhất: Các quá trình là khác biệt, yêu cầu các công cụ khác nhau để quản lý… Việc quản lý trang bị phần cứng với số lượng máy chủ lớn trở nên rất phức tạp và tốn công sức.

b. Máy chủ dạng phiến

Hạng mục	Thuyết minh
Tình hình sử dụng hiện nay	Khi cài đặt máy chủ mới trong phòng máy chủ của các tổ chức có qui mô, người dùng phải gắn nhiều thiết bị kết nối với máy chủ như bàn phím, chuột, màn hình, cáp nguồn, dây mạng và các kết nối với thiết bị lưu trữ. Nếu có nhiều máy chủ, đơn vị sẽ phải gắn rất nhiều thiết bị như vậy. Điều này đôi lúc không chỉ gây khó khăn mà còn chiếm nhiều

	không gian... Với những tồn tại như vậy trong hệ thống khi sử dụng server dạng rack-mount, dòng blade server ra đời với những tính năng nổi trội, khắc phục được những nhược điểm đồng thời nâng cao hiệu nâng, đáp ứng nhu cầu đưa ra trong hiện tại và dễ dàng mở rộng trong tương lai. Hệ thống máy chủ phiến gồm một bộ khung (chasis) có thể chứa từ 10 – 18 phiến, các máy chủ phiến, thiết bị quản lý và các cổng giao tiếp mạng, lưu trữ. Mỗi phiến là một máy chủ dạng gá (rack-mount) riêng biệt có kích thước khoảng 1U (~4,5cm) có từ 1 đến 4 CPU (2 đến 8 nhân), hỗ trợ khả năng bộ nhớ cao và có thể gắn 2 ổ cứng hay bản thân bộ khung máy cũng có thể chia sẻ hệ thống lưu trữ. Với chassis loại này vấn đề cấu hình cho các tác vụ chuyển đổi hay dự phòng rất thuận tiện. Hệ thống máy chủ phiến chỉ cần 1 bộ bàn phím, chuột, màn hình; hỗ trợ ít nhất 02 nguồn để đảm bảo dự phòng; và ít nhất 1 card giao tiếp mạng. Một số bộ khung máy chủ phiến còn cung cấp giao tiếp quang hay InfiniBand (InfiniBand hỗ trợ băng thông mạng trên 2,5Gbps, dùng giao thức IPv6) cho từng máy chủ phiến.
Ưu điểm	Bất kỳ tổ chức nào dùng trên 3 máy chủ nên cân nhắc dùng máy chủ phiến. Máy chủ phiến cho phép lắp dáp đơn giản, gọn gàng hơn nhiều so với máy chủ dạng rack-mount, không những thế còn giúp tiết kiệm không gian đặt máy chủ - trên một bộ khung máy chủ phiến có chiều cao khoảng 10U (~45cm) sẽ có từ 10 đến 16/18 phiến. Hiện nay, xu hướng thiết lập nhiều máy chủ ảo hóa trên một máy chủ vật lý đang trở thành trào lưu. Và với máy chủ phiến, nhà quản trị có thể kết hợp giải pháp ảo hóa để chạy nhiều hệ điều hành trên mỗi phiến. Thậm chí khi đang dùng từng máy chủ riêng biệt, máy chủ phiến là giải pháp thay thế hoàn hảo, giúp tiết kiệm nhiều chi phí quản lý hệ thống. Máy chủ phiến giúp giảm chi phí quản lý, quản trị dễ dàng nhiều tác vụ khác nhau, đơn giản hoá cáp nối cho trung tâm dữ liệu, tiết kiệm năng lượng và cho phép quản trị từ xa mà không cần lắp thêm thiết bị. Hệ thống máy chủ phiến có mức độ tin cậy cao hơn so với các máy chủ riêng biệt với các tùy chọn như nguồn dự phòng và các thành phần có tính sẵn sàng cao. **Tiết kiệm chi phí trong dài hạn:** Ưu điểm của blade là chúng có thể dùng chung nguồn điện và hệ thống làm mát. Nhờ vậy, máy chủ sẽ có

kích thước nhỏ gọn, mạnh mẽ và rẻ tiền hơn những hệ thống truyền thống như máy chủ trung tâm (mainframe) hay tập hợp các máy chủ (server farm).

Khả năng kết hợp: Hệ thống máy chủ Blade được phân chia thành các module được cô lập và có thể kết hợp dễ dàng với nhau, quản lý thông minh và được quản lý như 1 thiết bị, giúp giảm thời gian và chi phí khi xây dựng, duy trì và quản lý thiết bị. Ưu điểm về quản lý phần cứng của máy chủ phiến đem lại sự tiện lợi vượt trội so với các máy chủ đạng rack thông thường, đặc biệt với số lượng máy chủ lớn. Thay vì phải quản lý từ 10-18 máy chủ đơn lẻ với các cảnh báo riêng biệt, các thao tác thủ công trên từng máy một thì với máy chủ phiên, người quản trị chỉ cần thao tác duy nhất trên một khung chassis là có thể có mọi thông tin và hành động cần thiết cho các phiến máy chủ lắp trên đó.

Tiết kiệm không gian: Về mặt lý thuyết một tủ Rack tiêu chuẩn 42U có thể lắp tới 42 thiết bị máy chủ với kích thước 1U, nhưng thực tế chỉ có thể lắp được tối đa 25-30 thiết bị máy chủ với kích thước 1U, vì phần còn lại dùng cho các thành phần khác như patch panel (giá đấu nối mạng), khoảng cách trên dưới giữa các máy chủ (nhằm bảo vệ các máy và cách nhiệt, cách từ),…Với việc sử dụng thiết bị máy chủ Blade có kích thước chassis 10U, 01 tủ Rack có khả năng chứa tới 4 chassis các máy chủ Blade, mỗi chassis có khả năng hỗ trợ tối thiểu 10 máy chủ phiến, khả năng mở rộng trên 01 tủ Rack lên tới tối thiểu 40 máy chủ.

Khả năng mở rộng của hệ thống: Trong nền kinh tế cạnh tranh, việc

đầu tư các trang thiết bị phục vụ cho cơ sở hạ tầng CNNT cũng bị thu hẹp, chính vì vậy việc đầu tư trang thiết bị vừa đáp ứng được nhu cầu hiện tại và vẫn có khả năng mở rộng lớn phục vụ cho các mục tiêu trong tương lai với chi phí ban đầu thấp là một tiêu chí quan trọng trong việc lựa chọn thiết bị phù hợp. Việc ra đời các thiết bị máy chủ phiến hoàn toàn phù hợp với tiêu chí này. Đề cập tới khả năng mở rộng của các máy chủ Blade, có 02 tiêu chí được đề cập:

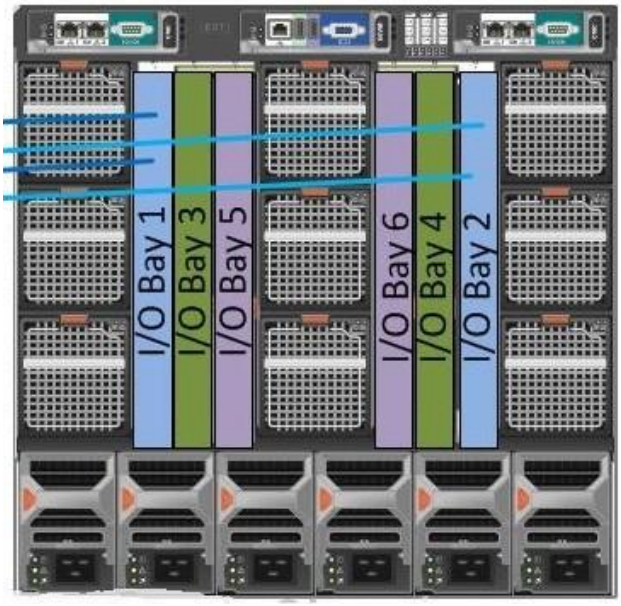
- Khả năng mở rộng các máy chủ phiến phục vụ ứng dụng:

+ Máy chủ Blade hiện tại phổ biến trên thị trường có kịch thước 10U Rack với khả năng mở rộng tối đa lên tới 18 máy chủ phiến. Với nhu cầu đầu tư ban đầu để đáp ứng được nhu cầu sử dụng hiện tại, giai đoạn đầu có thể mua từ 01-05 máy chủ phiến. Khi nhu cầu sử dụng tăng cao cộng với sự phát triển của các ứng dụng, người dùng có thể bổ xung thêm số máy chủ phiến một cách dễ dàng sao cho phù hợp với nhu cầu và sự phát triển đó. Chính vì vậy việc sử dụng máy chủ Blade được đánh giá rất linh hoạt trong các giai đoạn đầu tư và tối ưu về chi phí sử dụng trong khi đó khả năng mở rộng mạnh mẽ.

+ Ngoài ra, một máy chủ Blade còn hỗ trợ rất nhiều máy chủ phiến các loại, nhiều kích cỡ, năng lực xử lý cao hơn, hỗ trợ bộ nhớ CPU, RAM, HDD cao hơn, tương thích và đáp ứng một cách linh hoạt. Chính vì vậy với việc đầu tư ban đầu cho nhu cầu hiện tại, hệ thống hoàn toàn có thể đáp ứng được các mục tiêu xa hơn, đáp ứng được các nhu cầu về năng lực xử lý cao hơn gấp nhiều lần cho các ứng dụng và mục tiêu cao cấp hơn của các cơ quan, tổ chức.

- Khả năng mở rộng kết nối:

+ Việc sử dụng máy chủ cho nhiều chức năng trong hệ thống như: Kết nối xuống vùng lưu trữ, kết nối với hệ thống mạng hiện tại, với việc gia tăng số kết nối tới các vùng trong mạng theo nhu cầu sử dụng,

	một máy chủ Blade với khả năng hỗ trợ 04-06 các khe cắm I/O, việc mở rộng hệ thống kết nối vào ra từ máy chủ Blade đến các hệ thống mạng khác rất linh hoạt bằng cách cắm thêm các module kết nối vào các khe cắm I/O có sẵn trên backbone main của máy chủ. + Ngoài ra, một máy chủ Blade hỗ trợ nhiều khay cắm I/O với các tốc độ và chuẩn kết nối khác nhau, chính vì vậy song song với việc hỗ trợ số lượng nhiều khe cắm I/O trên mạch backbone, hệ thống còn hỗ trợ đa kết nối, đa tốc độ, đa tiêu chuẩn trên một mạch backbone. 

Đề xuất phương án

Dựa trên các phân tích trên về ưu nhược điểm của từng loại máy chủ, bên cạnh đó là chủ trương tiết kiệm chi phí thiết bị CNTT, đề xuất lựa chọn máy chủ cho dự án là máy chủ dạng rack (rack-mount server) mà vẫn đảm bảo tính sẵn sàng, khả năng mở rộng, quản trị.

2.3. Phân tích lựa chọn trang thiết bị phục vụ số hóa.

Số hóa tài liệu là quá trình chuyển đổi tài liệu dạng vật lý như giấy, ảnh, đồ vật sang dữ liệu dạng số để máy tính có thể đọc được. Các loại hình tài liệu (bao gồm dữ liệu dạng chữ, video, âm thanh, hình ảnh,...) sau khi qua công đoạn xử lý bằng các thiết bị chuyên ngành hoặc phần mềm chuyên dụng sẽ được tích hợp vào phần mềm ứng dụng để quản lý, tạo nên những cơ sở dữ liệu mở, dễ dàng tìm kiếm, trao đổi và chia sẻ kiếm thức một cách thuận tiện nhất.

Số hóa tài liệu ra đời chính là giải pháp khắc phục các nhược điểm của việc lưu trữ thông tin truyền thống, đưa ra cho doanh nghiệp phương án khai thác thông tin hiệu quả và nâng cao chất lượng công việc.

Phân tích các chủng loại máy scan cho ngành số hóa.

Máy quét tài liệu (Document Scanner): Đây là thiết bị phổ biến để quét tài liệu văn bản và hình ảnh một cách nhanh chóng và chất lượng cao. Máy quét tài liệu có thể kết nối trực tiếp với máy tính hoặc mạng để lưu trữ thông tin.

Máy quét phẳng (Flatbed Scanner): Tương tự như máy quét tài liệu, máy quét phẳng cũng quét tài liệu văn bản hoặc hình ảnh, nhưng với đầu đọc phẳng. Điều này cho phép quét các tài liệu không phẳng như sách, album ảnh, và đồ vật khác.

Máy quét di động (Portable Scanner): Là thiết bị nhỏ gọn và di động, thường kết nối không dây với máy tính hoặc điện thoại thông minh. Máy quét di động cho phép bạn quét tài liệu khi đang di chuyển hoặc không có máy tính gần.

Máy quét hình 3D (3D Scanner): Loại máy quét này tạo ra mô hình số hóa ba chiều của các đối tượng thực tế bằng cách quét chúng từ nhiều góc độ khác nhau. 3D Scanner thường được sử dụng trong ngành công nghiệp để tạo ra các mô hình in 3D hoặc phục vụ cho mục đích phân tích và thiết kế.

Máy quét mã vạch (Barcode Scanner): Dùng để quét mã vạch trên các sản phẩm, định danh và thu thập thông tin nhanh chóng. Máy quét mã vạch rất hữu ích trong bán lẻ, kho hàng và quản lý kiểm soát tồn kho.

Máy quét hình kỹ thuật số (Film Scanner): Đây là loại máy quét đặc biệt dùng để quét các tấm phim ảnh từ máy ảnh film, chuyển đổi chúng thành hình ảnh số và lưu trữ hoặc chỉnh sửa trên máy tính.

Máy quét tay (Handheld Scanner): Loại máy quét nhỏ gọn, cầm tay, thường được sử dụng để quét tài liệu hoặc hình ảnh từ các bề mặt lớn như bảng vẽ hoặc hình minh họa.

Đề xuất phương án:

Với nhu cầu thực tế của dự án là scan các tài liệu liên quan đến sơ đồ, đồ thị có tính chất khí tượng , thủy văn, vì vậy lựa chọn loại máy quét tài liệu.

3. THIẾT KẾ THI CÔNG

3.1. Yêu cầu, nhiệm vụ thiết kế

3.1.1. Yêu cầu về thiết kế

Để thực hiện được công tác tăng cường năng lực xử lý, lưu trữ chia sẻ , khai thác hiệu quả dữ liệu khí tượng thủy văn và đảm bảo an toàn an ninh thông tin cho hệ thống mạng Trung tâm dữ liệu của Tổng cục Khí tượng Thủy văn đáp ứng mục tiêu chung của dự án, nhiệm vụ thiết kế gói thầu này sẽ bao gồm:

- Phân tích hiện trạng, sự cần thiết đầu tư

–Thiết kế tổng thể hệ thống CNTT đáp ứng yêu cầu về quản lý, giám sát, lưu trữ, chia sẻ dữ liệu đáp ứng được các yêu cầu về nghiệp vụ và đảm bảo an toàn an ninh thông tin cho Trung tâm Dữ liệu của Tổng cục KTTV

- Đưa ra phương án bổ sung và nâng cấp hệ thống thiết bị bảo mật, máy chủ tại Tổng cục KTTV đảm bảo việc lưu trữ chia sẻ dữ liệu. Đảm bảo tích hợp hiệu quả với các hệ thống CNTT hiện có của Tổng cục KTTV theo hướng hiện đại hóa và tăng cường năng lực xử lý, tính toán

- Thiết kế chi tiết. Phần này nêu đề xuất các hợp phần liên quan đến CNTT trong khuôn khổ của dự án. Thiết kế chi tiết cho cụm thiết bị phần cứng; thiết kế chi tiết cho từng gói dịch vụ kỹ thuật đi kèm.
- Xây dựng biện pháp triển khai các thiết kế/giải pháp nói trên đồng thời đưa ra yêu cầu tối thiểu về thông số kỹ thuật thiết bị dự kiến đầu tư trong phạm vi gói thầu cũng như đối với dịch vụ triển khai lắp đặt, tích hợp cài đặt và cấu hình tổng thể hệ thống
- Từ các thiết kế trên đưa ra tổng dự toán chi tiết.

3.1.2. Nhiệm vụ thiết kế

- Thiết kế chi tiết các hạng mục cần mua sắm, lắp đạt bổ sung các thiết bị đảm bảo nâng cấp, tăng cường khả năng an toàn, bảo mật thông tin của hệ thống máy chủ và mạng của Tổng cục khí tượng thủy văn.

- Dự toán dịch vụ kỹ thuật cài đặt tối ưu hóa, tăng cường tính bảo mật của hệ thống CNTT hiện tại của Tổng cục KTTV

- Đưa ra chi tiết các yêu cầu về đào tạo hướng dẫn sử dụng.

- Đưa ra được yêu cầu về các dịch vụ bảo hành bảo trì hỗ trợ 24/7.

3.1.3. Hiện trạng hệ thống hạ tầng kỹ thuật

3.1.3.1. Hiện trạng hạ tầng kỹ thuật

3.1.3.1.1. Thiết bị

Qua khảo sát, hệ thống máy chủ và mạng của Tổng cục Khí Tượng Thủy Văn (TCKTTV) hiện có các thiết bị, bao gồm các chủng loại: thiết bị mạng, tường lửa, các máy chủ nghiệp vụ, máy chủ cơ sở dữ liệu Microsoft SQL Server, máy chủ cơ sở dữ liệu Oracle, hệ thống lưu trữ... Ngoài ra, Tổng cục cũng đang sử dụng một số hệ thống ảo hóa mà tiêu biểu là hệ thống sử dụng mã nguồn mở Ovirt, Promox và tiếp tục triển khai phần mềm quản lý dữ liệu tập trung (CDH) và phần mềm hỗ trợ dự báo thủy văn, hải văn (Delf-Few), các hệ thống ảo hóa này cho phép tạo được nhiều các máy chủ nghiệp vụ khác nhau, với nhiều hệ điều hành khác nhau, qua đó nâng cao năng lực đáp ứng yêu cầu công việc của ngành khí tượng thủy văn. Số lượng các thiết bị vật lý được thống kê trong Bảng 1.

Bảng 2. Danh mục các thiết bị chính của hạ tầng công nghệ thông tin tại TCKTTV

STT	Tên thiết bị	Model	Số lượng	Ghi chú
1	Core Switch	Cisco Nexus 7000 Series	2	Core Switch
	Core Switch	Cisco Nexus 9504 Series	2	Core Switch
2	Firewall	Cisco ASA 5580	1	Firewall Core & Server Farm, Firewall Internet
		Check Point 5400	1	
		Juniper SRX650	1	
		Cisco ASA 5540	1	
		Check Point 5900	1	
		Fortigate200E	1	
3	Router	Cisco ASR1001-X	2	Router Internet
		Cisco 2800	2	
		Cisco 3900 Series	1	
4	Switch	Cisco 2960	7	Switch Server Farm, Internet, Switch Access, Switch Access, Switch DMZ
		Cisco 3750	1	
		Cisco 3850	1	
		Edge-Core	2	
5	Balancing	DrayTeck Vigor 3900	1	Network Balancing
		Peplink 380	1	
		F5 Big-IP i2600	1	
		F5 Big-IP i2800	1	
6		Radware	1	DDos

	Thiết bị bảo vệ DDos	DefensePro 1016		
		Radware DefensePro 6-1	1	
7	Server	Dell R730	3	Voi IP, Data Server, GIS, Web, FTP, JAN0, JAN1, JAN2, SQL, Oracle, Máy chủ ứng dụng
		Dell R220	1	
		Dell R440	1	
		Dell R740	3	
		IBM x3650	18	
		IBM x3630	2	
		Fujitsu Primergy RX2540	1	
		NEC	4	
		Dell R330	3	
		Dell R430	3	
		Dell R630	3	
		HP DL360	2	
		HPE DL360 Gen10	10	
		Fujitsu PRIMERGY RX2520 M5	12	
		Fujitsu PRIMERGY RX1330 M4	2	
8	Storage	Hitachi VSP G200	1	
		Hitachi HUS 130	1	
		HPE MSA 2040	1	
		Fujitsu ETERNUS DX900S5	1	
9	Video Conference	Polycom	1	Video Conference
10	Hệ thống Blade Server	IBM BladeCenter H Type	1	Server
11	Hệ thống HPC	Cray XC40-AC	1	HPC System
12	SAN Switch	Dell PowerConnect Brocade 6505	2	SAN
13	Other	APC, Converter, Modem…		

a. Thiết bị mạng

Hầu hết các thiết bị mạng (bao gồm: thiết bị chuyển mạch, thiết bị định tuyến) đang sử dụng hiện nay tại Tổng cục đều của hãng CISCO. Đây là các thiết bị luôn cho độ ổn định mạng cao nhất trong các dòng sản phẩm cùng loại, có thể tận dụng tối đa dung lượng đường truyền. Đồng thời các thiết bị mạng của CISCO cho phép cung cấp nhiều tính năng quản lý truy cập, quản lý lưu lượng, thời lượng truy cập và khả năng mở rộng. Tuy nhiên, các thiết bị hạ tầng mạng (network) của Tổng cục KTTV hiện đã được đầu tư từ năm 2012, đến nay các thiết bị này đều đã cũ và hết thời hạn có thể bảo hành, bảo trì. Hơn nữa, năng lực của các thiết bị này không còn đáp ứng được yêu cầu của các trang thiết bị vừa mới được đầu tư trong các dự án gần đây như HPC, cơ sở dữ liệu Oracle, CDH và các phân hệ dự báo ... Cụ thể các thiết bị chính gồm:

Bộ chuyển mạch trung tâm (Core switch): Sử dụng 01 cặp Cisco Nexus 9504 serial (được trang bị năm 2022) làm thiết bị chuyển mạch trung tâm giúp cho hệ thống mạng tại Tổng cục có khả năng chịu tải lớn, hiệu năng cao phục vụ nhu cầu chuyển mạch chính trong toàn bộ hệ thống và điều chỉnh toàn bộ lưu lượng mạng trong hệ thống được xử lý ở tốc độ cao kèm theo tính sẵn sàng trong khả năng kết nối thực thi, phân phối cũng như bảo mật giữa các kết nối. Cisco Nexus 9000 serial có tốc độ chuyển mạch cao lên tới 15Tbps với kiến trúc dạng module, số lượng cổng kết nối tốc độ 1/10/40/100 GE. Vì đây là phần lõi cho hệ thống mạng của Trung tâm dữ liệu và đóng vai trò chuyển mạch trung tâm giữa Trung tâm Thông tin và Dữ liệu KTTV (HMDIC) với các phân vùng khác kết nối tới HMDIC, do đó việc sử dụng Cisco Nexus 9000 tại vị trí trung tâm của hệ thống dữ liệu của TCKTTV cho phép:

- Dễ dàng quản lý các phân vùng chuyên biệt và mở rộng trong tương lai.
- Tăng mức độ dự phòng hệ thống.
- Sử dụng tối đa các đường Uplink kết nối tới thiết bị Cisco Nexus 7000 do đó tăng băng thông hệ thống.

Cặp Core Switch này sẽ giúp cho hệ thống mạng hạn chế khả năng chịu lỗi, đảm bảo khả năng dự phòng và tăng cường tính sẵn sàng.

Thiết bị chuyển mạch (Switch): Hệ thống chuyển mạch của TCKTTV hiện nay đang sử dụng nhiều các model 2960S, 3750.. 24 port, tốc độ 10/100/1000 Mbs, là thiết bị chuyển mạch được sử dụng rộng rãi tại rất nhiều các hệ thống mạng từ mức độ trung bình trở lên. Dòng thiết bị này dễ dàng cấu hình và thuận tiện khi nâng cấp mở rộng

hệ thống. Tính ổn định của dòng sản phẩm này tương đối cao. Tất cả được đấu nối cho các phân vùng mạng trong toàn bộ Hệ thống mạng của TCKTTV và kết nối giữa các đơn vị trung tâm tại tòa nhà đến hệ thống máy chủ và ra ngoài Internet.

Thiết bị định tuyến (Router): Cisco 2800 series và 3900 series cho việc tổ chức định tuyến các gói dữ liệu giữa các mạng nội bộ với nhau, các mạng nội bộ và mạng Internet, WAN. Việc sử dụng 02 thiết bị định tuyến này là phù hợp đối với những hệ thống mạng vừa và nhỏ. Cisco 2800 hỗ trợ giao thức kết nối Ethernet, Fast Ethernet và khả năng cấp nguồn qua Ethernet (PoE). Router Cisco 2900 còn hội tụ đủ các giao diện mô-đun, cung cấp băng thông tăng dẫn đến đa dạng các khả năng phục hồi mạng và tùy chọn kết nối. Từ đó mang đến hiệu quả cao hơn trong quá trình sử dụng.

Tường lửa (Firewall): Tường lửa là nghiệp vụ kỹ thuật (thiết bị phần cứng, phần mềm hoặc là cả 2 kết hợp với nhau) được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập của một số truy cập không mong muốn vào hệ thống của các cá nhân, tổ chức, doanh nghiệp. Hệ thống công nghệ thông tin tại TCKTTV đang sử dụng các thiết bị tường lửa sau:

Cisco ASA 5540: cung cấp các dịch vụ bảo mật hiệu quả cao, VPN, kiểm tra và phòng chống thâm nhập, kiểm soát và bảo mật nội dung, thực hiện việc phòng chống virus, chống thư rác và ngăn chặn tập tin. Ngoài ra, Cisco ASA 5540 cung cấp khả năng hiển thị và kiểm soát chi tiết, bảo mật Web mạnh mẽ ngay tại chỗ hoặc trên đám mây, hệ thống phòng chống xâm nhập công nghiệp hàng đầu (IPS) để bảo vệ chống lại các mối đe dọa đã biết, bảo vệ toàn diện khỏi các mối đe dọa và phần mềm độc hại nâng cao.

Cisco ASA 5580: giám sát môi trường hệ thống, giới hạn người dùng VPN Remote Access. Với hiệu suất tường lửa 5 Gbps, 60.000 kết nối TCP mỗi giây và hỗ trợ tới 1 triệu kết nối. Cisco ASA 5580-40 cao cấp hơn với hiệu suất tường lửa lên tới 10 Gbps mỗi giây, 120.000 kết nối TCP mỗi giây và hỗ trợ lên tới 2 triệu kết nối. Kiến trúc đa lõi, đa bộ xử lý mang lại khả năng mở rộng triệt để cho bảo mật. Thiết bị tường lửa ASA được triển khai rộng rãi nhất trên thế giới với khả năng truy cập từ xa Cisco AnyConnect an toàn cao.

Check Point 5400, 5900: bảo vệ các cuộc tấn công mạng, các rủi ro từ Internet. Check Point 5400, 5900 cho phép kết nối tới hệ thống với băng thông lên tới 10Gb.

Juniper SRX650: chống virus, bảo mật ứng dụng, IPS, antispam, và tăng cường lọc Web. Nó hỗ trợ lên đến 7.0 Gbps tường lửa, 1,5 Gbps IPsec VPN, và 900 hệ thống phòng chống xâm nhập Mbps (IPS).

Fotigate200E: Với các tính năng, công nghệ bảo mật đa lớp để bảo vệ toàn diện cho dữ liệu, dịch vụ.

Ngoài ra hiện nay trên thiết bị định tuyến (Router) cũng có thể được cấu hình tường lửa nhằm bảo mật cho hệ thống.

Thiết bị cân bằng tải (Load Balancing): Hệ thống mạng của đang sử dụng Drayteck Vigor 3900 và Peplink Balance 380 phục vụ cho việc cân bằng tải đường truyền mạng người dùng tòa nhà. Drayteck Vigor 3900 hỗ trợ nhiều tính năng như: Multi VLAN, multi subnet, VPN, chống DoS/DdoS…Tuy nhiên đôi lúc sẽ cảm thấy rằng mạng chậm vì gói dữ liệu cần xử lý 2 lần, NAT Port phức tạp (bạn phải NAT 2 lần trên cả 2 thiết bị V3900 và router đứng trước). Thiết bị còn lại là PepLink Balance 380 với tính năng giúp tăng tốc độ dữ liệu mạng, độ tin cậy và tính linh hoạt. Hệ thống mới được trang bị thêm 02 thiết bị cân bằng tải ứng dụng F5 Big-IP i2600 và F5 BIG-IP i2800.

b. Thiết bị máy chủ và lưu trữ:

Máy chủ (Server): Hiện tại TCKTTV sử dụng nhiều dòng máy chủ như:

IBM x3650 và x3630. Ưu điểm của dòng máy chủ này:

- Khả năng mở rộng và nâng cấp dễ dàng.
- Có nhiều khay cắm ổ cứng 3.5 inch (tối đa lên tới 12 khay) nên IBM x3650 M4 cung cấp một giải pháp Server lưu trữ dung lượng cao.
- Hỗ trợ tốt cho ảo hóa và các ứng dụng khác. Nó hỗ trợ lên đến hai bộ xử lý Intel Xeon 8 lõi và thiết kế bộ nhớ mật độ cao với mười hai khe DDR3 DIMM.
- IBM x3650 M4 tích hợp bốn cổng Gigabit Ethernet và tùy chọn nhúng hai cổng 10 GbE nên dễ dàng cho phép nâng cấp tốc độ đường truyền trong quá trình truy xuất dữ liệu đến Server với chi phí nâng cấp không cao. Ngoài ra IBM x3650 M4 còn hỗ trợ lên tới 6 khe cắm PCI giúp cho khả năng nâng cấp và mở rộng dễ dàng.

Tuy nhiên, các dòng máy chủ trên vẫn còn một điểm hạn chế như sau:

- Khả năng hỗ trợ GPU (khả năng xử lý đồ họa) chưa cao

- Chưa đáp ứng đủ cho các phần mềm, ứng dụng nặng..

Dell R220, R440, R730 và R740. Trong đó Dell PowerEdge R730, R740 là dòng máy chủ thế hệ thứ 13,14 của Dell và mang lại hiệu suất ứng dụng nâng cao, dung lượng lưu trữ cao và nhiều tiềm năng mở rộng. Với thiết kế gồm các tính năng bảo mật tích hợp, Dell PowerEdge R740 là một trong những dòng máy chủ được lựa chọn nhiều nhất hiện nay. Hiệu suất cơ sở dữ liệu tốt hơn gấp mười lần với sự hỗ trợ cho NVDIMM và chipset mới của Intel cung cấp thêm 27% lõi hơn so với người tiền nhiệm của nó. Ba GPU hai chiều rộng hoặc sáu GPU đơn có thể được thêm vào hệ thống này để tăng cường khả năng xử lý. Với khả năng hỗ trợ hai bộ vi xử lý Intel Xeon Scalable với tối đa 28 lõi mỗi bộ xử lý thì máy chủ Dell R740 có khả năng thích ứng cao đối với mọi khối lượng công việc, phù hợp cho các ứng dụng:

- Ứng dụng tính toán hiệu năng cao
- Ứng dụng cho ảo hóa máy trạm với yêu cầu về xử lý đồ họa và dung lượng lưu trữ đa dạng
- Ứng dụng về ảo hóa lưu trữ như ScaleIO, vSAN
- Ứng dụng tương tác và chia sẻ công việc
- Ứng dụng triển khai cho các công nghệ chạy trện nền tảng Website
- Các ứng dụng của các nhà cung cấp dịch vụ, ứng dụng về tri tuệ nhân tạo và máy học (AI/ Machine Learning)
- Sử dụng cho nhu cầu tối ưu hóa tài nguyên cho các đám mây riêng (Private Cloud)….

Năm 2019, Tổng cục Khí tượng Thủy văn cũng mới được đầu tư thêm 12 máy chủ HP DL360 Gen 10, năm 2022 đầu tư thêm 14 máy chủ Fujitsu PRIMERGY RX2520 M5. Hiện tại máy chủ còn lại đang được sử dụng để cài đặt hệ thống ảo hóa Ovirt và ảo hóa Promox. Đến thời điểm hiện tại tất cả các máy chủ trong hệ thống của Tổng cục KTTV đều đã được sử dụng cho các công việc chuyên môn và không còn máy chủ cho phần mềm nghiệp vụ đầu tư mới cũng như không đảm bảo tính dự phòng cho hệ thống trong trường hợp xảy ra sự cố.

Hệ thống lưu trữ (Storage): Hệ thống lưu trữ được thiết kế dưới dạng SAN với bộ tủ đĩa Hitachi HUS 130. Đây là bộ tủ đĩa lưu trữ cung cấp hệ thống lưu trữ tầm trung (Midrange Level). Ưu điểm dòng sản phẩm này là:

- Kết hợp tốt nhất giữa hiệu suất ngẫu nhiên và tuần tự cho cả dữ liệu tệp và khối, HUS 130 có thể đạt được mục tiêu hiệu suất ở mức chi phí thấp nhất có thể.
- Chức năng lưu trữ cao cấp, chẳng hạn như cân bằng tải động và tự động phân tầng giúp mức hiệu suất có thể dự đoán được ngay cả trong môi trường tải thay đổi nhanh chóng.
- Cho phép triển khai lưu trữ cho tất cả các loại dữ liệu và dễ dàng phát triển để đáp ứng các yêu cầu mở rộng, chạy các ứng dụng quan trọng.
- Dễ dàng quản lý và sử dụng sẽ giúp cho việc quản trị hệ thống.

Nhược điểm:

- Tốc độ băng thông của hệ thống chỉ có thể đạt tốc độ tối đa lên đến 8Gbps, đây là điểm hạn chế khi hệ thống muốn nâng cấp băng thông lên 10Gbps hoặc cao hơn nữa.
- Việc thay thế các sản phẩm, thiết bị bị lỗi tương đối khó khăn do thị phần lưu trữ của Hitachi tại Việt nam không cao.

Hệ thống máy chủ phiến (Blade Server): Hệ thống máy chủ phiến của TCKTTV bao gồm các thiết bị:

- 01 Bladecenter: 4 Blade server
- 01 server IBM x3550
- 01 IBM System Storage DS3524
- 02 Switch Cisco

Hệ thống Blade của TCKTTV hiện nay đã có 4 blade và có thể nâng cấp tối đa lên thành 14 blade. Các balde có thể được tạo thành các máy chủ vật lý và máy chủ ảo và kết nối tới một bộ lưu trữ bên ngoài.

c. Các thiết bị khác

Ngoài các thiết bị nêu trên, hiện nay phòng máy chủ của TCKTTV đang vận hành thêm một số các thiết bị khác:

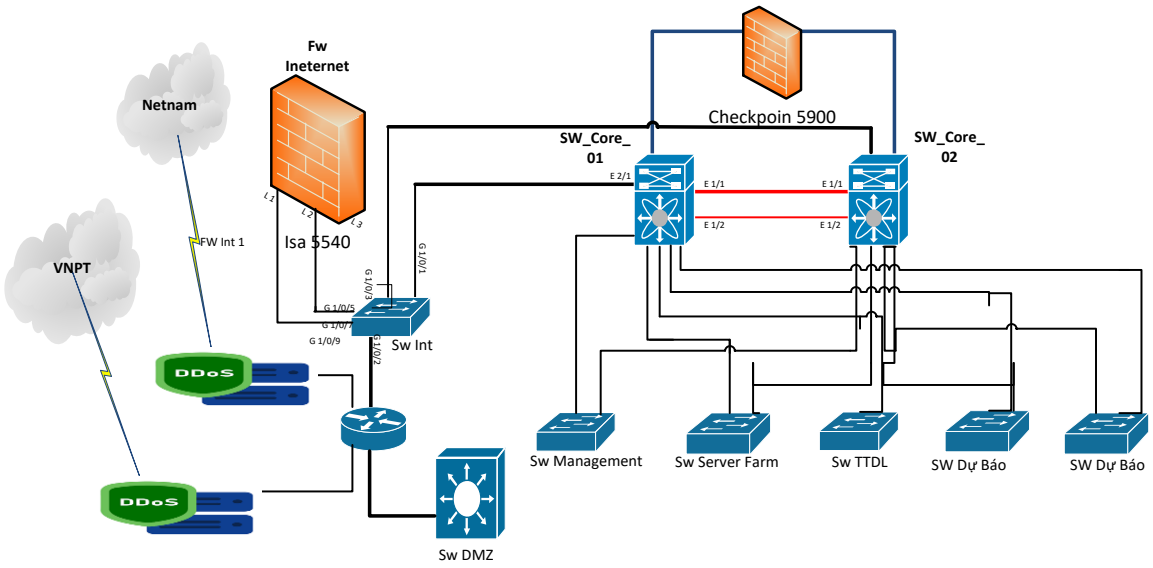
- Hệ thống tính toán hiệu năng cao (HPC) Cray XC40-AC với năng lực tính toán khoảng 76.8 Tflop để chạy các mô hình dự báo thời tiết số trị;
- Bộ họp trực tuyến Delta path và Polycom: Là 2 thiết bị về họp trực tuyến hàng đầu hiện nay, hỗ trợ các giải pháp: hội nghị truyền hình, phòng họp trực tuyến, điện thoại hội nghị…

- Bộ lưu điện APC: Công suất lưu điện hiện nay đủ đáp ứng cho toàn bộ thiết bị tại phòng máy chủ của Tổng cục.
- Bộ chuyển đổi, modem…

3.1.3.1.2. Hệ thống kết nối

a. Sơ đồ logic hệ thống:

Tương tự như mô hình hệ thống mạng của một doanh nghiệp, hệ thống kết nối tại TCKKTV cũng đã được xây dựng và thiết kế theo một mô hình mạng tiêu chuẩn như Hình 1, với các phân vùng như sau:



Hình 1. Sơ đồ logic hệ thống mạng Tổng cục KTTV

Vùng Internet: Tại vùng Internet đang chạy các thiết bị: 01 thiết bị định tuyến được kết nối đến 2 nhà cung cấp dịch vụ mạng Internet là VNPT và Netnam. Trên Internet có cấu hình VPN (mạng riêng ảo) nhằm bảo mật và bảo vệ sự riêng tư cho người dùng khi kết nối Internet. Chúng hạn chế rủi ro cho người dùng khi kết nối mạng và ngăn chặn các cuộc tấn công nguy hại từ bên ngoài. Phía sau thiết bị định tuyến được đặt và ASA5540.

Cấu hình hiện tại trên các thiết bị tại vùng Internet có thể tóm tắt và đánh giá qua một số điểm sau:

- Các thiết bị hoạt động đơn lẻ, không có tính dự phòng. Trong trường hợp một thiết bị gặp vấn đề, cả hệ thống sẽ bị gián đoạn, không đảm bảo độ ổn định và khả năng hoạt động liên tục. Đây là lỗi Single Point of Failure (SPOF).

- Định tuyến hiện sử dụng giao thức định tuyến động OSPF và định tuyến tĩnh. Trong đó định tuyến động OSPF khá phức tạp, nhiều cấu hình không cần thiết gây khó khăn cho người quản trị hệ thống kiểm soát. Ngoài ra, hiện chưa có cơ chế bảo vệ định tuyến, là điểm yếu gây gián đoạn dịch vụ trong quá trình vận hành.
- Sử dụng 02 thiết bị tường lửa không cùng loại nên hiệu năng sử dụng không cao do hoạt động đơn lẻ, không có phương án dự phòng. Thiết bị Check point đang hoạt động như 1 thiết bị chuyển mạch và không tối ưu. Chính sách bảo mật trên thiết bị còn lại chưa được thiết lập để đảm bảo an toàn thông tin cho hệ thống.
- Hầu hết đang sử dụng 1 link để kết nối giữa 2 thiết bị. Không có cơ chế dự phòng cho các link kết nối.
- Hệ thống mạng bên trong sử dụng các link 10Gb nhưng tất cả lưu lượng đi ra Internet lại tập trung qua 1 link 1Gb nối với thiết bị chuyển mạch Internet gây hiện tượng nghẽn cổ chai cho toàn hệ thống.

Vùng DMZ: Đây là nơi chứa những Server và cung cấp những dịch vụ (Directory service, DNS, DHCP, File/Print Sharing, Web, Mail, FTP, Proxy…) cho những máy tính ở trong mạng nội bộ cũng như những thiết bị khác từ mạng bên ngoài vào. Là bước cuối mà những gói dữ liệu từ phía bên trong mạng nội bộ đi qua trước khi truyền ra ngoài Internet, và cũng là nơi đầu tiên mà những gói tin từ bên ngoài đến trước khi được vào mạng nội bộ.

Do tính chất quan trọng của vùng DMZ nên việc bảo mật cho vùng này cần được chú trọng. Mặc dù có 1 thiết bị tường lửa được đặt trước vùng DMZ để kết nối với mạng nội bộ và ra ngoài Internet, nhưng do hiệu năng thiết bị tường lửa hiện tại không đảm bảo tính bảo mật nên nguy cơ các cuộc tấn công mạng từ bên ngoài và từ chính trong mạng nội bộ đối với vùng này hoàn toàn có thể xảy ra. Ngoài ra với việc chỉ sử dụng 01 thiết bị chuyển mạch cho khu vực trên sẽ không đảm bảo tính sẵn sàng và hiệu năng cao. Hầu hết đang sử dụng 1 link để kết nối giữa 2 thiết bị, chưa có cơ chế dự phòng cho các link kết nối.

Bên cạnh đó, việc sử dụng chung đường kết nối giữa vùng cung cấp dịch vụ và truy cập internet của người dùng khiến cho dòng lưu lượng đi qua chung 1 hệ thống (Router, Switch, Firewall,…) xử lý => Có thể dẫn đến kịch bản lưu lượng truy cập internet của người dùng tạo ra ảnh hưởng (chậm, rớt gói, sai phạm…) đến các dịch

vụ được cung cấp ra bên ngoài của Tổng cục KTTV, khó tối ưu được các chính sách tuân thủ an toàn thông tin riêng rẽ cho từng loại dịch vụ, máy chủ và người dùng.

Vùng Core Switch: Cisco Nexus 9504 Series đang được cấu hình các vlan với các tên khác nhau như:, TTTL, DDB, DCK, TTQG, TTCNTT1, TTCNTT2…

Vùng Server Farm: Là nơi đặt các máy chủ không trực tiếp cung cấp dịch vụ cho mạng Internet. Các máy chủ triển khai ở vùng mạng này là SQL Server, Oracle Server, GIS, máy chủ chạy các phần mềm dự báo…Ngoài ra đây là nơi tập trung các máy chủ lưu trữ, hệ thống lưu trữ cơ sở dữ liệu, thông tin dự báo…Vì vậy, có thể coi đây là phân vùng tối mật và quan trọng bậc nhất TCKTTV. Các thiết bị của vùng này bao gồm:

- 01 thiết bị tường lửa Checkpoint 5900
- Các thiết bị chuyển mạch (Switch Access)
- Các máy chủ cơ sở dữ liệu
- Hệ thống lưu trữ SAN

Vì là vùng tối mật và quan trọng bậc nhất đối với các hoạt động của TCKTTV nên việc bảo mật và tăng cường giám sát đối với khu vực này vô cùng thiết yếu. Khu vực vực này hiện được phân ra thành 01 phân vùng riêng với vùng Core Switch và có thiết bị tường lửa bảo vệ. Tuy nhiên, cũng giống như các thiết bị tường lửa khác trong hệ thống mạng thì hiện nay thiết bị này chưa được thiết lập đầy đủ các chính sách để đảm bảo an toàn thông tin cho hệ thống.

Ngoài ra, tại vùng Server Farm đang sử dụng hệ thống lưu trữ SAN phục vụ cho việc lưu trữ và back up số liệu, dữ liệu KTTV. Hệ thống lưu trữ SAN Hitachi với dung lượng hữu dụng khoảng hơn 30TB đang được phân chia thành nhiều volume phục vụ cho công tác lưu trữ. Ngoài ra năm 2022 thông qua dự án WB 8 Tổng cục được đầu tư hệ thống SAN Fujitsu với tổng dung lượng lưu trữ hiệu dụng khoảng 250TB (28TB SSD, 60TB HĐ 10K, 183 TB 7.2K)

Vùng User: Cụ thể ở đây là các Trung tâm, phòng ban của Tổng cục kết nối đến phòng Máy chủ thông qua các thiết bị chuyển mạch (Switch Access). Người dùng đang truy cập đến hệ thống, chưa được kiểm soát qua hệ thống tường lửa dẫn đến nguy cơ xâm nhập thất thoát dữ liệu cao.

Hạ tầng phòng máy chủ: Trong thời gian gần đây, Tổng cục Khí tượng Thủy văn đã được đầu tư hạ tầng Trung tâm Dữ liệu tương đối hiện đại, đảm bảo điều kiện môi

trường hoạt động cho các thiết bị công nghệ thông tin trong Trung tâm. Hạng mục mới đầu tư này đã tạo ra nền tảng tốt về môi trường hoạt động và tính toán cho Tổng cục Khí tượng Thủy văn, đáp ứng được nhu cầu hiện tại và trong một vài năm sắp tới nếu không có sự tăng trưởng đột biến về số lượng thiết bị được đầu tư trong Phòng máy chủ.

3.1.3.2. Đánh giá hiện trạng

Qua thực tế khảo sát hiện trạng tại phòng máy chủ TC KTTV, tư vấn đưa ra một số điểm hạn chế về hệ thống CNTT của Tổng cục như sau:

Về vận hành:

Tổng cục KTTV đang sử dụng rất hạn chế một số phương thức khác nhau, ứng với từng loại thiết bị/ vendor để giám sát riêng rẽ công việc vận hành hệ thống. Khiến bộ phận công nghệ thông tin gặp nhiều khó khăn trong việc giám sát tổng thể hoạt động của toàn bộ hệ thống (thiết bị, dịch vụ, ứng dụng) và bị động nếu có các sự số xảy ra. Việc thiếu một hệ thống lưu trữ nguồn log hoạt động (của thiết bị) cũng kéo dài thời gian xử lý sự cố khi phải truy cập vào từng hệ thống riêng rẽ để tìm kiếm nguồn gốc gây lỗi, dẫn đến việc dịch vụ có thể gián đoạn hàng giờ đồng hồ (đến hàng ngày) nếu có sự cố nghiêm trọng xảy ra.

Về hiện trạng an toàn thông tin:

Tổng cục KTTV đã được trang bị khá cơ bản các giải pháp kiểm soát hệ thống tuy nhiên vẫn chưa đủ khả năng đảm bảo an toàn dữ liệu tuyệt đối trong bối cảnh mà tình hình an ninh mạng ngày càng căng thẳng, khi các tổ chức kinh tế, tài chính, chính phủ, an ninh quốc gia… phải đối mặt với hang nghìn cuộc tấn công mỗi ngày trên toàn thế giới, và tại Việt Nam có ít nhất gần 100 cuộc tấn công mỗi ngày (Theo số liệu của VNCERT). Bên cạnh đó, các cuộc tấn công an ninh mạng ngày càng tinh vi hơn, do hacker ngày càng có trình độ, được đầu tư, và có tổ chức thic ác giải pháp an ninh hiện tại vẫn chưa đủ để đáp ứng nhu cầu an toàn thông tin dữ liệu của đơn vị.

Các tấn công có chủ đích (Targeted Attacks) và các mối đe dọa bền bỉ phức tạp (Advanced Persistent Threat APT) đang nhanh chóng trở thành một tiêu chuẩn mới của các mối đe dọa an ninh mạng – bao gồm các cuộc tấn công tập trung, có chủ đích được thiết kế riêng để xâm nhập vào các cơ quan chính phủ nhằm tìm kiếm các thông tin có giá trị, bí mật quốc phòng, và truy xuất vào các hệ thống nội bộ bên trong

Đơn vị cần xây dựng hệ thống nền tảng điều hành an ninh bảo mật đủ mạnh để giám sát phát hiện và ngăn chặn được hầu hết các tấn công trên không gian mạng nhằm khai thác các lỗ hổng trên các ứng dụng cũng như thiết bị tin học trong mỗi hệ thống mạng của các tổ chức

Về thiết bị:

Nhiều thiết bị đã end of life (EoL) và end of sale (EoS) (Firewall ASA 5580, ASA 5540, Router Cisco 2800, Router 3900…), do đó sẽ không trang bị được các gói hỗ trợ cũng như cập nhật các bản vá bảo mật mới từ hãng nếu có bất kỳ sự cố gì xảy ra với phần cứng/phần mềm của thiết bị. Ngoài ra, tình trạng an ninh mạng hiện nay đang rất phức tạp, Việt Nam được ghi nhận là quốc gia có nhiều cuộc tấn công mạng. Vì vậy, các thiết bị EoL và EoS không có các bản vá lỗi định kỳ sẽ là mục tiêu để các hacker tấn công, phá hoại và gây ảnh hưởng tới sự an toàn và uy tín của đơn vị.

Các thiết bị Firewall, chạy đơn lẻ (cụ thể hơn: Firewall cho khu vực Internet đang được sử dụng là 01 thiết bị ASA 5440, Router cho khu vực Internet đang được sử dụng là 01 thiết bị Cisco 3900, nên không có cơ chế Backup và High Availability (HA) dẫn đến không đảm bảo về tính sẵn sàng và trong các trường hợp xảy ra sự cố.

Firewall SRX650 sử dụng module phát hiện và ngăn chặn Virus của Sophos, khi bật tính năng thì hiệu năng của Firewall giảm mạnh còn 350Mbps. Thêm nữa tính năng Virus trên Firewall chỉ hạn chế được một số loại Virus trên mạng, không thể chuyên sâu như các hệ thống Antivirus trên Endpoint.

Firewall Fotigate200E có đầy đủ các tính năng IPS, Antivirrus tuy nhiên cấu hình thiết bị thấp, hiệu năng thiết bị không đủ đáp ứng được các yêu cầu.

Thiết bị mạng nói chung đều đã trang bị từ năm 2012, EoS nên sẽ ảnh hưởng tới hiệu năng chuyển mạch trung tâm của thiết bị, khả năng mở rộng module khi số lượng thiết bị đấu nối của hệ thống tăng thêm.

Các thiết bị lưu trữ tại Data Center của Tổng cục Khí tượng Thủy văn hiện đã được đầu tư từ lâu, đến nay hầu hết dung lượng lưu trữ của các thiết bị này đã được sử dụng hết nên hiện tại một số dữ liệu có kích thước lớn đang phải tạm thời sử dụng vùng lưu trữ của hệ thống HPC (~280 TB). Đối với thiết bị lưu trữ dữ liệu SAN mới được đầu tư năm 2022 hiện tại phân vùng dung lượng ổ cứng đọc ghi tốc độ cao (SSD và 10K) đã phân bổ hết, hiện tại chỉ còn phân vùng lưu trữ dữ liệu sử dụng ổ cứng tốc độ đọc ghi 7.2K. Với thông số kỹ thuật như vậy phân vùng ổ cứng này chỉ phù

hợp với việc lưu trữ dữ liệu lâu dài mà không phù hợp trong việc truy xuất và đọc ghi dữ liệu tốc độ cao.

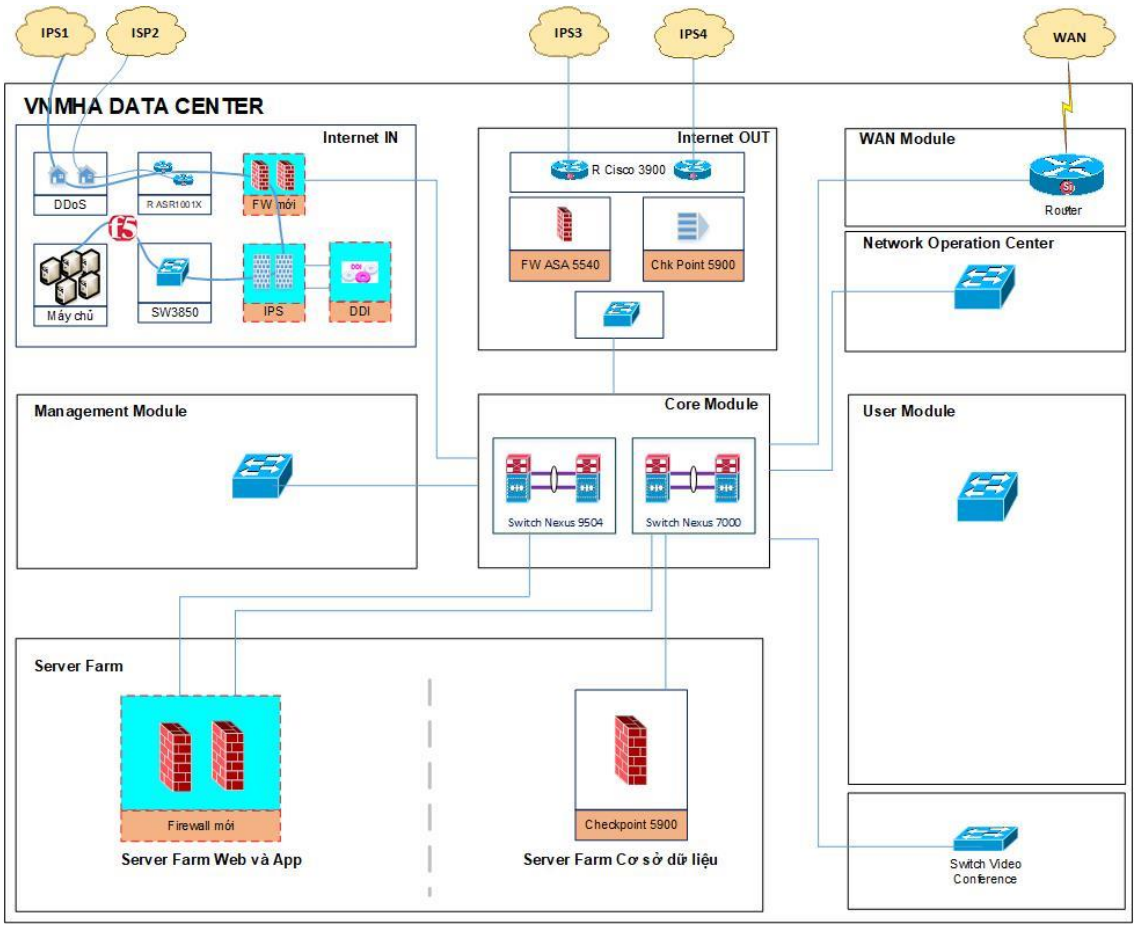
Một số thiết bị mới được đầu tư năm 2019, 2022 đã sử dụng đường truyền cáp quang 10Gbps để kết nối nội bộ nhưng hầu hết các kết nối giữa các thiết bị trong hệ thống hiện tại đặc biệt là kết nối giữa các thiết bị ở các phân vùng khác nhau, khu vực Internet vào/ra dữ liệu vẫn chỉ mới được sử dụng đường truyền 1Gbps dẫn tới việc không đáp ứng được tốc độ truyền/nhận, đọc/ghi dữ liệu của hệ thống vào một số thời điểm.

3.2. Thiết kế kế hệ thống

3.2.1. Thiết kế tổng thể

3.2.1.1. Thiết kế logic hệ thống

Căn cứ trên hiện trạng cũng như nhu cầu thực tế của Tổng cục KTTV, tư vấn đề xuất mô hình logic kết nối các thiết bị hiện có của Tổng cục KTTV và các thiết bị dự kiến được đầu tư trong dự án thể hiện qua sơ đồ logic như sau:



Hình 2. Sơ đồ thiết kế logic

Như vậy, trong khuôn khổ của dự án đối với thiết bị, kế thừa toàn bộ hạ tầng hiện tại và bổ sung thêm 02 phần chính: (1) Phần thiết bị đảm bảo an toàn an ninh thông tin; và (2) phần thiết bị máy chủ phục vụ triển khai CSDL Big data;

Về quy mô thiết kế, các thiết bị được thiết kế là một thành phần quan trọng của Trung tâm Dữ liệu Tổng cục Khí tượng Thủy văn. Ngoài việc tăng cường đảm bảo an toàn an ninh thông tin cho Trung tâm Dữ liệu cũng cần phải tăng cường năng lực chung cho ngành KTTV đáp ứng các nhu cầu ngày càng cao trong thực tiễn, vì vậy yêu cầu về hệ thống bảo mật, máy chủ có cấu hình mạnh, có khả năng mở rộng nhằm đáp ứng mục tiêu chung của dự án nói riêng và khả năng phát triển của cơ sở dữ liệu dùng chung trong tương lai.

Mô hình mạng mới của Tổng cục KTTV phải được thiết kế dựa trên kiến trúc mạng hiện tại của Tổng cục nhằm tối ưu hóa hạ tầng và tiết kiệm chi phí đầu tư. Tuy nhiên hệ thống phải đảm bảo tính sẵn sàng kể cả việc xảy ra hỏng hóc đối với một thiết bị phần cứng, đảm bảo truy cập liên tục tốc độ cao cho phân vùng CSDL. Do đó việc thiết kế hệ thống tại Tổng cục KTTV phải đáp ứng một số các yêu cầu sau:

- Có dự phòng cho các thiết bị quan trọng (có từ 2 thiết bị trở lên chạy đồng thời đảm bảo không xảy ra gián đoạn hệ thống khi có lỗi xảy ra trên 1 thiết bị. Các thiết bị quan trọng phải có 2 nguồn điện. Firewall, IPS Router phải cấu hình chạy ở chế độ Cluster, HA;

- Thiết bị mạng, thiết bị bảo mật phải tính đến phương án có thể tận dụng lại thiết bị hiện có tại Trung tâm Dữ liệu của Tổng cục KTTV nhằm giảm chi phí đầu tư;

- Máy chủ có cấu hình tương đối đủ mạnh để có thể chạy các phần mềm ứng dụng, phần mềm CSDL, tương thích với các hệ điều hành Windows, linux có kiến trúc 64 bit, hỗ trợ ảo hóa, dung lượng ổ cứng lưu trữ có thể chứa dữ liệu trong vòng 36 tháng, yêu cầu tốc độ truy cập cao đáp ứng việc truy xuất khai thác dữ liệu tốc độ nhanh;

- Việc triển khai hệ thống không cho phép gián đoạn hệ thống mạng ảnh hưởng đến nghiệp vụ của các đơn vị trong Tổng cục;

Căn cứ vào thiết kế tổng thể, thiết kế logic hệ thống, dựa trên hiện trạng về kết nối mạng, hạ tầng cơ sở, các thiết bị hiện có và nhu cầu quản lý, vận hành, lưu trữ khai thác dữ liệu của Tổng cục KTTV. Tư vấn đề xuất các hợp phần trong đó bao gồm các hợp phần về tăng cường trang thiết bị phần cứng (PC) và các dịch vụ kỹ thuật kèm theo (DV) cụ thể:

Bảng 3. Phạm vi đầu tư

TT	Hạng mục đầu tư	Ghi chú
1	**Tăng cường an toàn thông tin**	

TT	Hạng mục đầu tư	Ghi chú
1.1	Firewall thế hệ mới	Bảo vệ 02 khu vực trọng yếu là + Internet In + Server Farm
1.2	Thiết bị phòng chống tấn công có chủ đích	Tăng cường bổ sung thêm cho khu vực Internet IN. Đảm bảo các mối nguy cơ không thể xâm nhập được vào hệ thống.
	+ Thiết bị phát hiện các mối nguy cơ	
	+ Thiết bị ngăn chặn các mối nguy cơ	
1.3	Nâng cấp cặp Switch Core Cisco Nexus 7000 + 44 cặp module quang + 44 cáp quang 20m[A1]	Tăng cường năng lực xử lý từ 1G lên 10G cho các máy chủ BigData và đấu nối vật lý với Firewall mới.
2	**Thiết bị CSDL Big data**	
2.1	Máy chủ Name node	
2.2	Máy chủ Data node	
2.3	Máy chủ ứng dụng	
3	**Dịch vụ**	
3.1	Dịch vụ triển khai, lắp đặt và cài đặt thiết bị	
3.2	Dịch vụ tối ưu theo tiêu chuẩn CIS	
3.3	Dịch vụ nâng cấp firmware (hoặc OS) thiết bị	
3.4	Đào tạo chuyển giao công nghệ	

3.2.1.2. Yêu cầu thiết bị firewall

Firewall được trang bị tại phân vùng Internet In và Server Farm phải là Firewall thế hệ mới. Thiết bị phải tương thích với các thiết bị hiện có, đặc biệt phải hoạt động rất ổn định bởi vì vừa thực hiện ngăn chặn tấn công từ vùng Firewall nhưng lại phải đáp ứng yêu cầu tương thích về tốc độ với cặp Switch Core hiện tại. Thiết bị phải hỗ trợ đa dạng các chuẩn vật lý cũng như các tiêu chuẩn an toàn thông tin mới nhất. Ngoài ra để giảm thiểu các rủi ro về chuỗi cung ứng, trong thiết kế hệ thống cần hướng đến đa dạng hóa các vender (hãng cung cấp) đối với các giải pháp, hệ thống, thiết bị bảo mật nói chung và thiết bị Firewall nói riêng. Vì vậy trong khuôn khổ của dự án cần đầu tư các thiết bị nằm ngoài danh mục thiết bị đang sử dụng tại Tổng cục Khí tượng Thủy văn. Yêu cầu tối thiểu như sau:

Bảng 4. Yêu cầu tối thiểu thiết bị Firewall

TT	Nội dung yêu cầu	Đáp ứng tối thiểu
1	Số cổng dữ liệu đồng hỗ trợ	8 x 1G/2.5G/5G/10G
2	Số cổng dữ liệu quang 10 Gbps hỗ trợ	12 x 1G/10G SFP/SFP+
3	Cổng quang tốc độ cao	4 x 25G SFP28 4 x 40G/100G QSFP+/QSFP28
4	Kết nối high availability	2 x 1G SFP, 1 x 40G QSFP+
5	Thông lượng tường lửa ứng dụng (Application)	43.0 Gbps
6	Thông lượng Threat Prevention	26 Gbps
7	Thông lượng IPSEC	21 Gbps
8	Số phiên kết nối VPN Site 2 site	4,000
9	Số lượng phiên kết nối đồng thời	3.5 M
10	Số lượng phiên kết nối tạo mới / giây	270,000
11	Số chính sách (security rules)	30,000
12	Số NAT rules	6,000
13	Số vùng an ninh (security zone)	4,000
14	Số virtual router	20
15	Số tường lửa ảo (virtual system) có sẵn và có thể mở rộng tối đa	10/20
16	Số virtual wire	2,048
17	Số phiên kết nối Remote VPN cho người dùng từ xa	15,000
18	Tính năng HA	HAactive/active, active/passive, HA clustering
19	Nguồn / Cấu trúc thiết bị	02 nguồn AC / Rackmount

3.2.1.3. Yêu cầu thiết bị phòng chống tấn công có chủ đích (ATP)

Thiết bị phòng chống tấn công có chủ đích (ATP) phải là thiết bị chuyên dụng. Là tuyến phòng thủ cuối cùng trước khi đi vào hệ thống. Cho nên, thiết bị này phải giám

sát đa dạng các giao thức truyền thông trên mạng, phát hiện ngay cả khi mối nguy hại chưa đi vào hệ thống. Yêu cầu tối thiểu như sau

Bảng 5. Yêu cầu tối thiểu thiết bị phòng chống tấn công có chủ đích

TT	Nội dung yêu cầu	Đáp ứng tối thiểu
1	**Thiết bị ngăn chặn mối nguy cơ (IPS)**	
1.1	Dạng thiết bị	Dạng thiết bị độc lập lắp Rack
	Cổng dữ liệu quang 10 Gbps	≥ 08 cổng kèm theo các loại linh kiện Card, SFP/SFP+ để đảm bảo tốc độ 10Gbps, hỗ trợ bypass
	Cổng dành riêng cho quản trị	Có cổng quản trị riêng
	Độ trễ	< 40 µs
	Thông lượng IPS	≥ 03 Gbps
	Số lượng session/connection đồng thời hỗ trợ tối đa	≥ 120,000,000 sessions
	Số lượng kết nối mới trên giây hỗ trợ	≥ 650,000
	Hỗ trợ chế độ tương thích cấu hình	Giải pháp TPS phải hỗ trợ chế độ tự tương thích cấu hình, cho phép cảnh báo hoặc vô hiệu các rule không hiệu quả trong trường hợp hệ thống bị nghẽn
	Chế độ hoạt động	Hỗ trợ chế độ hoạt động bypass ở lớp 2 để bypass lưu lượng mạng ngay cả khi thiết bị đang hoạt động, hoặc lúc phần mềm bị lỗi như hỏng firmware, hay bộ nhớ bị lỗi.
	Hỗ trợ các cơ chế HA	active/active, active/passive
	Tính năng bảo mật	Phải hỗ trợ phát hiện xâm nhập/tấn công/traffic nguy hiểm dựa trên sigatures,

TT	Nội dung yêu cầu	Đáp ứng tối thiểu
		protocol anomaly, lổ hổng bảo mật, trafffic anomaly
	Khả năng tích hợp với công cụ dò quét lỗ hổng bảo mật	Công cụ quản trị tập trung các thiết bị IPS hỗ trợ import đánh giá về các lổ hổng bảo mật từ bên thứ ba như Qualys, Rapid7, Nessus.., từ đó cho phép nhà quản trị áp đặt các rule vá ảo lỗ hổng bảo mật nhanh chóng
	Khả năng tích hợp với công cụ dò quét lỗ hổng bảo mật	Công cụ quản trị tập trung các thiết bị IPS hỗ trợ import đánh giá về các lổ hổng bảo mật từ bên thứ ba như Qualys, Rapid7, Nessus.., từ đó cho phép nhà quản trị áp đặt các rule vá ảo lỗ hổng bảo mật nhanh chóng
2	**Thiết bị phát hiện mối nguy cơ (DDI)**	
1.1	Dạng thiết bị	Hardware box kèm phần mềm chuyên dụng
1.2	Năng lực	Xử lý phân tích được lưu lượng tối thiểu 1 Gbps
1.3	Số lượng sandbox hỗ trợ	4
1.4	Tính năng bảo mật	- Giám sát hơn 100 giao thức mạng trên tất cả các cổng dịch vụ mạng nhằm phát hiện mã độc - Khả năng phát hiện mã độc với sandbox tích hợp sẵn (sandbox có khả năng tùy chỉnh)
1.5	Môi trường giả lập (sandbox) cần hỗ trợ các hệ điều hành	Windows, Linux, Mac OS
1.6	Khả năng phân tích các file nén có đặt mật khẩu (password-protected files)	Cho phép import password để phân tích file nén được bảo vệ bởi password nhằm phát hiện malware

3.2.1.4. Yêu cầu nâng cấp cặp Switch Core Cisco Nexus 7000

Nhằm đáp ứng yêu cầu tốc 10G của hệ thống BigData cần thiết phải nâng cấp cặp switch Core Cisco Nexus 7000 có sẵn tại tổng cục. Cặp switch core này có hỗ trợ tốc độ 1Gbps/10Gbps, vì vậy, cần nâng cấp đồng bộ các module quang tốc độ 10G, cụ thể như sau:

Bảng 6. Yêu cầu nâng cấp 01 cặp switch Core Cisco Nexus 7000

TT	Nội dung yêu cầu	Số lượng	Đáp ứng tối thiểu
1	Module quang	44 cặp	10Gbps SPF+ Cổng LC chuẩn Ethernet
2	Cáp quang LC-LC	44 sợi	20m

3.2.1.5. Yêu cầu về dịch vụ

a) Dịch vụ 1: Triển khai, lắp đặt và cài đặt thiết bị mới được đầu tư trong dự án

Các thiết bị và phần mềm trang bị cho gói thầu này áp dụng những công nghệ mới nhất, tiên tiến nhất, một số thiết bị là chuyên dụng. Để đảm bảo làm chất lượng cần thiết phải mua dịch vụ triển khai, lắp đặt và cài đặt thiết bị ban đầu phù hợp với các yêu cầu do TCKTTV đưa ra.

b) Dịch vụ 2: Dịch tối ưu hóa, cập nhật hệ điều hành mới cho các thiết bị công nghệ thông tin tại Tổng cục Khí tượng Thủy văn.

- Tối ưu hóa và đảm bảo cấu hình thiết bị được quy chuẩn theo CIS
  - Khảo sát cấu hình hiện tại của các thiết bị mạng trong Trung tâm dữ liệu;
  - So sánh, đánh giá với quy chuẩn;
  - Lập kế hoạch;
  - Triển khai thực hiện.
- Nâng cấp hệ điều hành: Nâng cấp OS các thiết bị thuộc Trung tâm dữ liệu TCKTTV trong phạm vi được chủ đầu tư đưa ra bao gồm nhưng không giới hạn: Router, Switch, Load-Balancer, Firewall, DDoS…. Yêu cầu trong quá trình nâng cấp cập nhật đảm bảo không gián đoạn dịch vụ, cụ thể:
  - Khảo sát hệ điều hành hiện tại và đưa ra các khuyến nghị;
  - So sánh, đánh giá sự phù hợp với quy chuẩn, sự phù hợp với các khuyến nghị của hãng;
  - Lập kế hoạch;
  - Triển khai thực hiện.
- Rà soát và tối ưu hóa các chính sách "rule/policy" trên các thiết bị Firewall

Bao gồm các thiết bị của dự án cũng như các thiết bị Firewall, thiết bị cân bằng tải, Router đang hoạt động để đồng bộ xuyên suốt hệ thống chính sách trên toàn hệ thống.

- Khảo sát các chính sách hiện tại và thực hiện tài liệu hóa;
- Rà soát nhu cầu của người dùng đối với các luồng dữ liệu cần đi qua Firewall;
- Thiết kế và đồng bộ chính sách theo Phương án tối ưu;
- Lập kế hoạch triển khai trên tất cả các thiết bị Firewall;

- Đồng bộ, tối ưu cấu hình hệ thống

Thực hiện đối với tất cả các thiết bị trong Trung tâm dữ liệu nhằm đảm bảo việc triển khai xuyên suốt

- Rà soát cấu hình hiện tại của các thiết bị "Middleware devices" bên trong Trung tâm dữ liệu;
- Cấu hình các tính năng liên quan trên các thiết bị đang vận hành thuộc Trung tâm dữ liệu nhằm đảm bảo vận hành xuyên suốt của các nhóm thiết bị mới;

c) Dịch vụ 4: Đào tạo chuyển giao công nghệ

Để đảm bảo làm chủ hệ thống đặc biệt là các hạng mục mới bổ sung, cần phải tổ chức các khóa đào tạo chuyển giao công nghệ tại TCKTTV. Bao gồm các nội dung tối thiểu:

- Hướng dẫn lắp đặt, cài đặt, vận hành thiết bị
- Hướng dẫn quản trị, cấu hình hệ thống
- Hướng dẫn khai thác hệ thống

Ghi chú: Các khóa đào tạo phải bao gồm các tài liệu do chính hãng cung cấp.

3.2.2. Thiết kế tăng cường an toàn thông tin

Căn cứ theo đánh giá hiện trạng trên, xác định 02 phân vùng cần ưu tiên tăng cường bảo vệ trước như sau:

- Phân vùng Internet In: Đây là phân vùng cung cấp các dịch vụ thiết yếu cho toàn bộ hệ thống. Là chốt chặn cuối cùng các mối nguy hại, luôn thường trực mối nguy hại trong hệ thống. Vì vậy, cần thiết phải chủ động phòng thủ bằng thiết bị chuyên dụng. Như vậy, firewall bảo mật tại phân vùng này gồm:

Bảng 7. Thiết bị tại phân vùng Internet In

TT	Chủng loại	Số lượng	Ghi chú
1	Firewall thế hệ mới	02	Trang bị mới
2	ATP		
	+ Thiết bị phân tích mối nguy hại (DDI)	01	Trang bị mới
	+ Thiết bị ngăn chặn mối nguy hại (ISP)	02	Trang bị mới

Ghi chú: Lưu lượng sạch (đã được lọc qua Firewall) từ Firewall đi vào đến vùng Internet IN vào lúc tải cao chiếm băng thông khoảng 100Mps. Như vậy, phương án sử dụng Firewall 1G đứng trước phân vùng này làm nhiệm vụ đóng, mở cổng là hoàn toàn khả thi.

- Phân vùng ServerFarm: Tương tự như phân vùng Internet IN, thiết bị trang bị từ năm 2018. Đây là phân vùng, có ý nghĩa đặc biệt quan trọng liên quan trực tiếp đến dữ liệu và các ứng dụng hệ thống. Cho nên, cần phải tăng cường bảo vệ bằng firewall thế hệ mới. Bên cạnh đó, ưu tiên bảo vệ phân vùng dữ liệu bằng cách sử dụng lại Firewall Checkpoint 5900.

Bảng 8. Danh sách thiết bị tại phân vùng Server Farm

TT	Chủng loại	Số lượng	Ghi chú
1	Firewall thế hệ mới	02	Trang bị mới
2	Firewall Checkpoint 5900	01	Thiết bị đã có, bảo vệ riêng cho Server Farm database

Như vậy, phân vùng này chỉ mở các cổng dịch vụ của cơ sở dữ liệu (ví dụ như cổng 1521/Oracle hoặc 1433/MSSQLServer). Tốc độ 1G khi truy vấn CSDL là hoàn toàn khả khi. Bởi vì, tốc độ đọc ghi giữa máy chủ CSDL với SAN/Storage chạy qua SAN Switch (không chạy qua switch 1G) cho nên hoàn toàn không ảnh hưởng đến tốc độ xử lý dữ liệu của hệ thống.

Bảng 9. Bảng tổng hợp danh sách thiết bị bảo mật

TT	**Chủng loại**	**Số lượng**	**Ghi chú**
1	**Internet In**		
1.1	Ddos DefensePro	02	Đã có sẵn
1.2	Firewall thế hệ mới	02	Trang bị mới
1.3	ATP		
	+ Thiết bị phân tích mối nguy hại (DDI)	01	Trang bị mới
	+ Thiết bị ngăn chặn mối nguy hại (IPS)	02	Trang bị mới
2	**Internet Out**		
2.1	Check Point 5900	01	Đã có, giữ nguyên
3	**Server Farm**		
3.1	Firewall thế hệ mới	02	Trang bị mới
3.2	Firewall Checkpoint 5900	01	Đã có, bảo vệ riêng Server Farm DB

3.2.3. Phương án tối ưu thiết bị

Như đã phân tích đánh giá trong mục hiện trạng, không chỉ thiết bị bảo mật, các thiết bị mạng, máy chủ cũng cần được rà soát tối ưu theo tiêu chuẩn bảo mật CIS mới nhất và cần nâng cấp firmware (hoặc hệ điều hành) theo khuyến nghị của hãng sản xuất để phát huy hết năng lực thiết bị. Bên cạnh đó, tiêu chuẩn CIS không sử dụng giao

thức định tuyến động OSPF (chỉ sử dụng giao thức định tuyến tĩnh). Cho nên, giải quyết được các vướng mắc đang gặp phải.

Bảng 10. Danh mục thiết bị cần tối ưu

TT	Thiết bị	Ghi chú
1	Switch	Thực hiện trước khi lắp đặt thiết bị mới
2	Router	Thực hiện trước khi lắp đặt thiết bị mới
3	Firewall và thiết bị bảo mật	Thực hiện trước khi lắp đặt thiết bị mới
4	Các thiết bị máy chủ	Thực hiện trước khi lắp đặt thiết bị mới
5	Cân bằng tải	Thực hiện trước khi lắp đặt thiết bị mới

Cấu hình kết nối giữa các phân vùng trong hệ thống sẽ được đi qua tối thiểu 01 firewall, các phân vùng quan trọng như datatabase, Internet In sẽ đi qua 02 firewall của các hãng khác nhau. Bên cạnh đó, các nhân sự vận hành của các phân vùng này cũng sẽ khác nhau để đảm bảo dữ liệu đi vào các phân vùng quan trọng bắt buộc phải đi qua 02 thiết bị và phải được mở rule bằng 02 nhân sự khác nhau.

Bảng 11. Bảng quy hoạch địa chỉ mạng IP

TT	VLAN	Dải IP	Gateway
1	Vlan 14 – TTCNTT2	10.151.3.0/25	10.151.3.1
2	Vlan 15 – Cao không	10.151.4.0/24	10.151.4.1
3	Vlan 60 – Mạng lưới	10.151.5.0/24	10.151.5.1
4	Vlan 100 – Management	10.152.1.64/26	10.152.1.126
5	Vlan 110 – LMS_ACS	10.152.1.0/29	10.152.1.1
6	Vlan 115 – CN_ServerFarm	10.152.0.8/29	10.152.0.12
7	Vlan 513 – Gateway-User	10.151.2.128/25	10.151.2.129

- Video Conference sử dụng 2 dải IP 10.1.0.0/28 và 10.151.37.128/25 để phục vụ kết nối với nhà mạng và cung cấp kết nối đến các thiết bị đầu cuối sử dụng hội nghị truyền hình.
- Management sử dụng VLAN 100 và dải mạng IP 10.152.1.64/26 để quản trị.
- Các End User tương ứng với các phòng ban được cấu hình các VLAN khác nhau, sử dụng default gateway ảo trên cặp Switch Core (Cặp switch core sử dụng giao

thức HSRP để đảm bảo dự phòng).

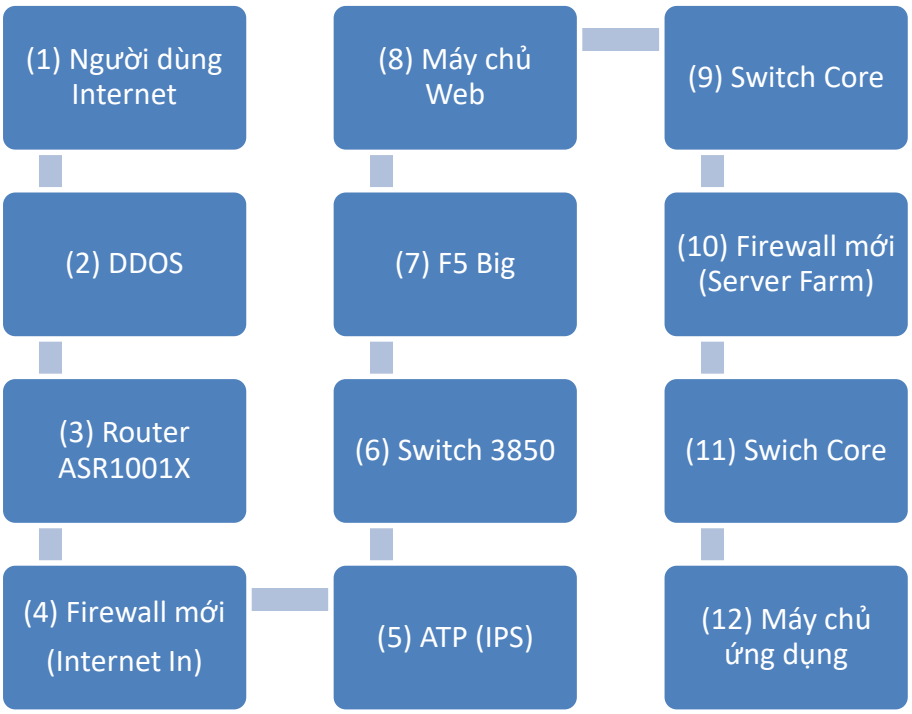
- TW sử dụng dải IP 10.152.0.48/29 để tham gia định tuyến với dải IP 10.151.0.0/23 dành cho các endpoint.
- Cao không sử dụng VLAN 60 với dải địa chỉ 10.151.5.0/24 dành cho các endpoint.
- User CNTT sử dụng VLAN 513 với dải IP 10.151.2.128/25 dành cho các endpoint.

Ghi chú: Các file cấu hình sẽ được sao lưu định kỳ của trên máy chủ FPT trong hệ thống.

3.2.4. Mô tả một số luồng dữ liệu quan trọng

3.2.4.1. Cung cấp dịch vụ truy cập từ ngoài Internet

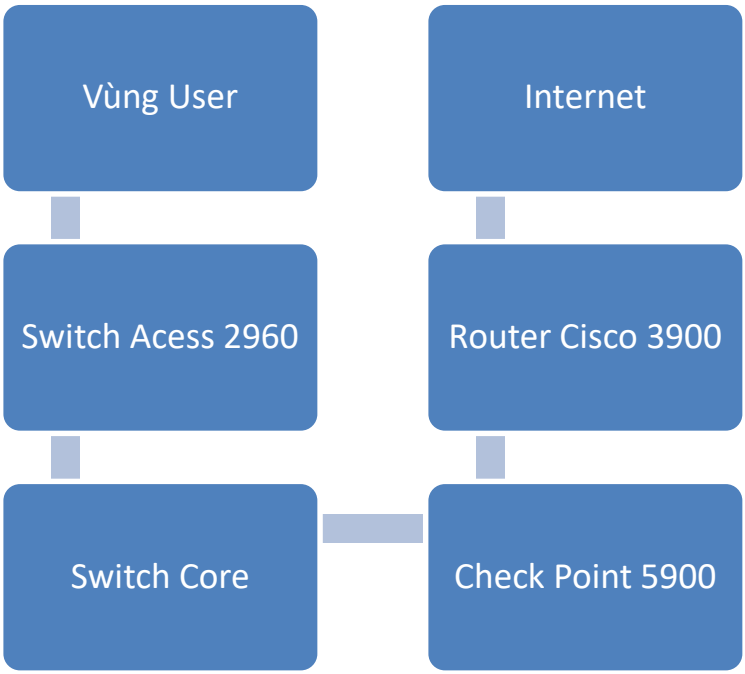
Đây là luồng dữ liệu incoming, hướng dữ liệu sẽ đi từ người dùng từ ngoài Internet vào trong hệ thống. Ví dụ như người dùng ngoài Internet truy cập Webiste Tổng cục hoặc truy cập các dịch vụ chuyên ngành của Tổng cục.



Hình 3. Sơ đồ luồng dữ liệu từ ngoài Internet vào hệ thống

3.2.4.2. Cung cấp dịch vụ kết nối từ vùng User ra ngoài Internet (Outgoing)

Đây là luồng dữ liệu outgoing, hướng dữ liệu sẽ đi trong hệ thống ra ngoài Internet, ví dụ như người dùng từ vùng User truy cập Internet.

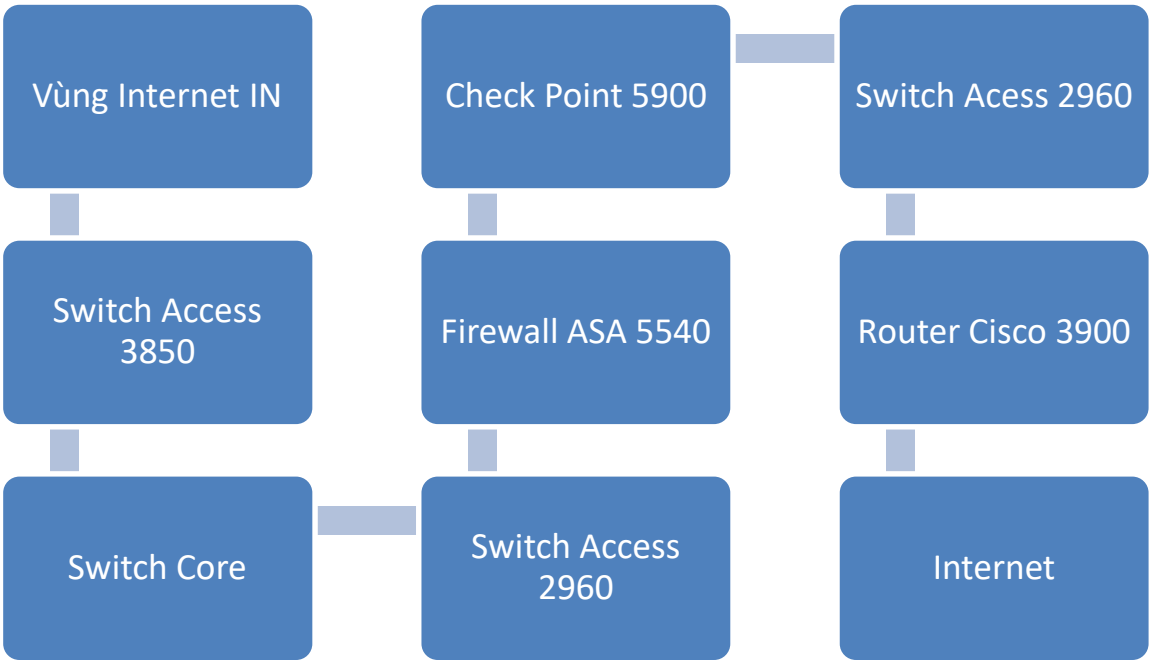


Hình 4. Sơ đồ luồng dữ liệu từ vùng User truy cập Internet

3.2.4.3. Cung cấp dịch vụ kết nối từ vùng Internet IN ra ngoài Internet

Tại phân vùng này các máy chủ vẫn cần phải kết nối Internet để sử dụng các dịch vụ như: Dịch vụ đồng bộ thời gian (NTP), dịch vụ cập nhật bản vá (Internet Proxy) từ nhà sản xuất, dịch vụ Email.

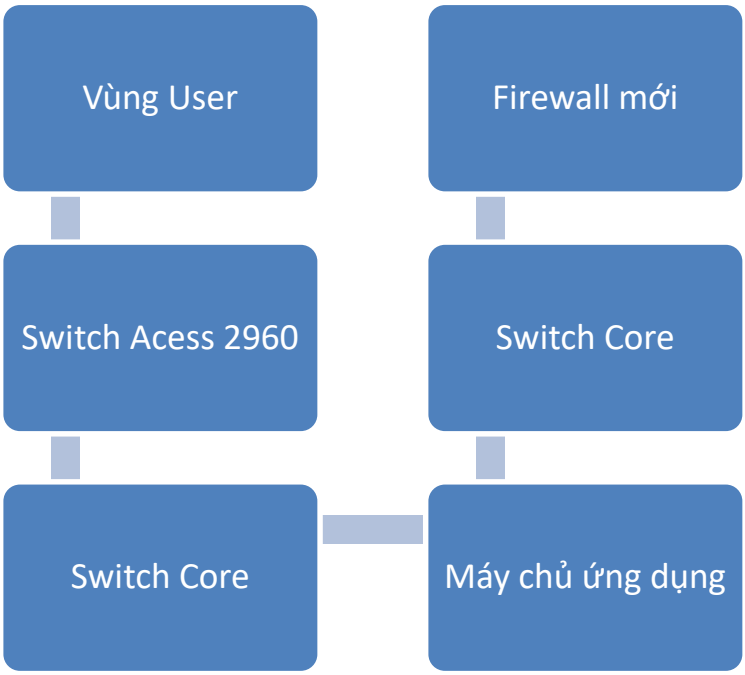
Mặc dù vùng này có kết nối đến 02 ISP, tuy nhiên, kết nối 02 ISP chỉ dành cho chiều Incoming. Đối với chiều outgoing, vùng này sẽ đi qua Swich core đến vùng Internet Outgoing và đi ra ngoài Internet.



Hình 5. Luồng dữ liệu từ vùng Internet IN đi ra ngoài Internet

Luồng dữ liệu này khi đi đến Firewall sẽ lọc các domain, cổng, tiếp theo sẽ liệu sẽ gửi đến Check Point 5900 để lọc các mã độc trước khi đi ra ngoài Internet thông qua ISP.

3.2.4.4. Luồng dữ liệu từ vùng User vào vùng ứng dụng



Hình 6. Luồng dữ liệu từ vùng User đi vào ứng dụng

3.2.5. Thiết kế trang bị hệ thống Bigdata

3.2.3.1 Nhu cầu về lưu trữ dữ liệu tại Tổng cục.

Bảng 12. Tính toán dữ liệu về nhu cầu lưu trữ tại tổng cục

STT	Danh mục dữ liệu	Dung lượng ngày Trung bình (GB/ngày)	Dung lượng hàng năm (GB)	Ghi chú
	Dữ liệu quan trắc nội địa	1.1	401.5	
	Dữ liệu quan trắc ngoại địa	2.3	839.5	
	Dữ liệu vệ tinh địa tĩnh	6	2190	
	Dữ liệu vệ tinh cực	8	2920	
	Dữ liệu rada	25	9125	10 rada, mỗi Rada 2.5GB/ngày
	Dữ liệu định vị set	0.3	109.5	
	Dữ liệu dự báo	1.5	547.5	Phục vụ cho việc đánh giá và quản lý dự báo.
	Dữ liệu quan trắc thu nhận Mạng lưới KTTV	0.8	292	
	Dữ liệu khác		200	
	Tổng cộng		16.625	
	Tỉ lệ dư liệu phát triển hàng năm : 115%			
	Tổng dung lượng cần thiết cho 03 năm		**57,356.25**	

3.2.3.2 Đinh cỡ hệ thống.

3.2.5.1.1. Dung lượng lưu trữ

Để tính dung lượng ổ cứng lưu trữ cho mỗi máy data node trong mạng Hadoop sử dụng HDFS, cần lưu ý rằng HDFS lưu trữ dữ liệu theo cơ chế chia nhỏ và phân tán trên các node. Theo mặc định, Hadoop sử dụng cơ chế chia nhỏ dữ liệu thành các khối (block) có kích thước mặc định là 128MB (tuy nhiên, có thể điều chỉnh).

Dựa vào lượng dữ liệu là 20TB, ta cần tính số lượng khối dữ liệu và sau đó xác định dung lượng ổ cứng cần thiết cho mỗi máy data node. Trong trường hợp này, ta sẽ giả định mỗi khối có kích thước 128MB.

- Tính số lượng khối dữ liệu 1 TB = 1024 GB do vậy với lượng dữ liệu 20 TB = 20 * 1024 GB = 20480 GB

với khối có kích thước là 128MB = 0.128 GB

- Số lượng khối dữ liệu = 20480 GB / 0.128 GB = 160,000 khối

- Tính dung lượng ổ cứng cần thiết cho mỗi máy data node Vì HDFS lưu trữ các bản sao (replicas) của dữ liệu, mặc định là 2 bản sao. Điều này đảm bảo tính sẵn sàng và đáng tin cậy của dữ liệu trong môi trường phân tán.

Mỗi máy data node cần lưu trữ một bản sao của các khối dữ liệu này.

Dung lượng ổ cứng cần thiết cho mỗi máy data node = Tổng dung lượng dữ liệu / Số lượng máy data node. Dung lượng ổ cứng cần thiết cho mỗi máy data node = 60TB / 5 = 12TB với 20% lưu trữ để trống để đảm bảo hiệu năng truy suất dữ liệu nên sẽ cần dung lượng cho mỗi node là 14,4TB. Vậy, để lưu trữ lượng dữ liệu 20TB trên 5 máy data node sử dụng HDFS với công nghệ Hadoop, mỗi máy data node cần có ít nhất 14,4TB dung lượng ổ cứng lưu trữ.

Các đề xuất về kích thước và điều chỉnh khác nhau dựa trên loại triển khai, dựa trên các yếu tố triển khai nhất định trong miền và môi trường Hadoop, ta có thể triển khai ở mức cơ bản với các tiêu trí triển khai tích hợp kỹ thuật dữ liệu như sau:

Số lượng người dùng hoạt động

Số lượng người dùng đang làm việc trên kho dữ liệu mô hình trong quá trình thiết kế, sử dụng công cụ Analyst hoặc chạy các công việc kỹ thuật dữ liệu trong môi trường chạy thời gian gốc hoặc Hadoop tại bất kỳ thời điểm nào.

Số lượng đồng thời của các ánh xạ được đẩy xuống

Tổng số ánh xạ đang chạy trên các động cơ Blaze, Spark hoặc Hive mà được gửi đồng thời đến Dịch vụ tích hợp dữ liệu.

Số lượng đối tượng trong kho dữ liệu mô hình

Tổng số đối tượng thiết kế và chạy thời gian trong kho dữ liệu mô hình. Ví dụ, đối tượng dữ liệu, ánh xạ, luồng công việc và ứng dụng.

Số lượng ứng dụng triển khai

Tổng số ứng dụng được triển khai trên tất cả Dịch vụ tích hợp dữ liệu trong miền Hadoop.

Số lượng đối tượng mỗi ứng dụng

Tổng số đối tượng của tất cả các loại được triển khai là một phần của một ứng dụng duy nhất.

Tổng lượng dữ liệu vận hành

Tổng lượng dữ liệu được xử lý trong môi trường Hadoop tại bất kỳ thời điểm nào.

Tổng số nút dữ liệu

Tổng số nút dữ liệu trong cụm Hadoop.

yarn.nodemanager.resource.cpu-vcores

Một thuộc tính trong tệp yarn-site.xml trên cụm Hadoop xác định số lõi ảo cho các container.

yarn.nodemanager.resource.memory-mb

Một thuộc tính trong tệp yarn-site.xml trên cụm Hadoop xác định bộ nhớ vật lý tối đa có sẵn cho các container.

Yếu tố triển khai	**Triển khai ở mức tiêu chuẩn**
Số người dùng đang hoạt động đồng thời	10
Số lượng ánh xạ đẩy xuống đồng thời	1000 – 2000
Số đối tượng trong kho Model	< 20,000
Số lượng ứng dụng đã triển khai	< 100
Số đối tượng trên mỗi ứng dụng	50 -100
Tổng khối lượng dữ liệu vận hành trên cụm máy tính	>500 GB
Đối với các trường hợp sử dụng xử lý hàng loạt	1 triệu

Môi trường Hadoop

Bảng sau đây chứa các hướng dẫn về các yếu tố triển khai trong môi trường Hadoop

Yếu tố triển khai	**Triển khai ở mức tiêu chuẩn**
Tổng số nút dữ liệu	9
yarn.nodemanager.resource.cpu-vcores	24
yarn.nodemanager.resource.memory-mb	>49152 MB

Khuyến nghị về định cỡ máy chủ

Bảng sau liệt kê các yêu cầu phần cứng tối thiểu và tối ưu cho cụm Hadoop

Phần cứng	**Triển khai ở mức tiêu chuẩn**
Tốc độ CPU	2 - 2.5 GHz
Lõi CPU logic hoặc ảo	24
Tổng bộ nhớ hệ thống	128 GB
Không gian đĩa cục bộ cho yarn.nodemanager.local-dirs1	500 GB
Kích thước khối DFS	128 MB
Hệ số sao chép HDFS	3
Dung lượng đĩa	3 TB
Tổng số đĩa cho HDFS	8 (sử dụng Raid5 với 1 ổ đĩa parity&1 ổ spare)
Tổng dung lượng HDFS trên mỗi nút	14,4 TB
Số node data	5
Tổng dung lượng HDFS trên cụm	60 TB
Dung lượng HDFS thực tế (có sao chép)	3 TB
/tmp mount	20 GB
Yêu cầu dung lượng đĩa cài đặt	22 GB
Băng thông mạng (Ethernet)	10 Gbps (bonded channel)

3.2.5.1.2. Máy chủ riêng phân vùng Database (DB zone)

Phân vùng Database dành riêng cho việc lưu trữ dữ liệu và phân tách với các phân vùng mạng khác để đảm bảo tính bảo mật dữ liệu. Phân vùng dữ liệu chỉ cho phép truy cập từ Phân vùng ứng dụng, Phân vùng admin với một số dịch vụ cần truy cập vào dữ liệu thông qua firewall.

- ***Máy chủ Name Node 1, 2***

Máy chủ Name node 1 cài đặt các ứng dụng Master chịu trách nhiệm thu nhận thông tin, điều phối và điều khiển các máy chủ data node. Đây là máy chủ quan trọng trong hệ thống Bigdata, nếu máy chủ này dừng hoạt động thì sẽ làm dừng toàn bộ hệ thống Bigdata, vì vậy máy chủ Name node 1 được dự phòng bởi máy chủ Name node 2 đóng vai trò là Slave hay Secondary. Khi máy chủ 1 dừng hoạt động thì máy chủ Name node 2 sẽ đóng vai trò làm Master và hệ thống vẫn có thể hoạt động. Các ứng dụng cài đặt trên máy chủ Name node 1 bao gồm:

- HDFS Name Node
- Mapreduce JobTracker
- ES Master node
- Hbase HMaster node
- Yarn Resource Manager
- ZooKeeper
- Ambari agent
- Apache Oozie

Kết luận: để đảm bảo sự hoạt động tốt và đáp ứng yêu cầu của hệ thống, Vì vậy cấu hình đề xuất CPU 24core và RAM 64 GB.

Kết nối mạng Ethernet cần đảm bảo yếu tố truy xuất nhanh với băng thông rộng 10GB/s và ít nhất 2 port, trong đó 1 port dự phòng.

- ***Các máy chủ DataNode***

Các máy chủ Data node đóng vai trò chính trong việc lưu trữ dữ liệu. Ngoài ra còn đảm nhiệm việc xử lý dữ liệu Mapreduce. Đồng thời các data node được cài đặt các ứng dụng worker để giám sát tài nguyên data node. Các ứng dụng được cài đặt bao gồm:

- HDFS data node
- Mapreduce TaskTracker
- ES Data node
- Yarn node Manager
- Hbase Region Server
- Ambari agent

Với nhiệm vụ chính lưu trữ dữ liệu thì Datanode cần thiết phải đảm bảo được các thông số sau:

- Storage có dung lượng lưu trữ 18TB dành riêng cho dữ liệu và 0.5TB dành cho OS và cài đặt ứng dụng.
- Storage đảm bảo chạy với bộ điều khiển RAID 5E để đảm bảo tính dự phòng của ổ cứng lưu trữ.
- Tần suất truy cập dữ liệu nhiều do chứa lượng lớn dữ liệu từ các ứng dụng database như HDFS, Hbase, ES, Mapreduce vì vậy IPOS cần đạt tối thiểu 20000.

Các ứng dụng database yêu cầu cao về CPU và RAM để đảm bảo các hoạt động nền và đáp ứng nhanh các yêu cầu truy vấn dữ liệu vì vậy cấu hình đề xuất CPU 48core và RAM 256 GB.

Storage đảm bảo chạy với bộ điều khiển RAID 5 để đảm bảo tính dự phòng của ổ cứng lưu trữ.

Kết nối mạng Ethernet cần đảm bảo yếu tố truy xuất nhanh với băng thông rộng 10GB/s và ít nhất 4 port, trong đó 1 port dự phòng.

3.2.5.1.3. Máy chủ riêng phân vùng Ứng dụng (App Zone).

➢ ***Máy chủ ứng dụng (APP server)***

Máy chủ ứng dụng (APP server) đóng vai trò cung cấp các ứng dụng cơ sở và cho phép truy cập, triển khai và vận hành các ứng dụng lập trình. Các ứng dụng cơ sở để truy cập vào cơ sở dữ liệu như: HiveService, Sqoop, Flume hoặc triển khai các ứng dụng phân tích và xử lý dữ liệu như: Storm, Spark, Mahout, Drill, PIG. Hoặc ứng dụng giám sát hệ thống như Ambari web. Các ứng dụng cài đặt bao gồm:

- Apache Spark driver application
- HiveService
  Apache Drill
- Apache PIG
- Apache Mahout
- Apache SQOOP
- Apache FLUME
- Apache Storm Master
- Apache Spark cluster Manager
- Ambari web
- Apache Tomcat

Các ứng dụng chạy không đòi hỏi storage lưu trữ dữ liệu lớn chỉ lưu trữ log với 0.8T và 0.5T dành cho OS và cài đặt các ứng dụng. Storage đảm bảo chạy với bộ điều khiển RAID 5 để đảm bảo tính dự phòng của ổ cứng lưu trữ.

Kết nối mạng Ethernet cần đảm bảo yếu tố truy xuất nhanh với băng thông rộng 10GB/s và ít nhất 4 port, trong đó 1 port dự phòng.

Do chạy đồng thời nhiều ứng dụng vì vậy yêu cầu dung lượng RAM 128G và CPU 48 core

- ***Máy chủ Worker***

Các máy chủ triển khai các ứng dụng worker đóng vai trò chạy các tác vụ xử lý dữ liệu, tính toán dạng Data Stream hoặc Data Flow. Các ứng dụng cài đặt bao gồm:

- Kafka worker
- Apache Storm worker
- Apache Spark Worker
- Ambari agent

Với nhiệm vụ đặc biệt xử lý và tính toán cao và đặc biệt là xử lý tính toán trên bộ nhớ RAM thì các máy chủ worker cần được trang bị CPU mạnh mẽ với 48 core và dung lượng RAM 128G.

Các ứng dụng chạy không đòi hỏi storage lưu trữ dữ liệu lớn chỉ lưu trữ log với 0.8T và 0.5T dành cho OS và cài đặt các ứng dụng. Storage đảm bảo chạy với bộ điều khiển RAID 5 để đảm bảo tính dự phòng của ổ cứng lưu trữ.

Kết nối mạng Ethernet cần đảm bảo yếu tố truy xuất nhanh với băng thông rộng 10GB/s và ít nhất 4 port, trong đó 1 port dự phòng.

3.2.3.3 Danh mục đề xuất cấu hình máy chủ và thiết bị mạng cho hệ thống Bigdata gồm

No		Tên máy chủ	Số lượng máy chủ	Chức năng, ứng dụng được cài đặt trên máy	RAM (GB)	CPU (Core)	Storage (TB)	RAID	Ethernet
1	**Máy chủ riêng phân vùng Database (DB zone)**		**7**						
1.1		Name Node 1	1	HDFS Name Node Mapreduce JobTracker ES Master node Hbase HMaster node Yarn Resource Manager ZooKeeper Ambari agent Apache Oozie	64	24	0.96	RAID 1	4 Port 10Gb
1.2		Name Node 2	1	HDFS Secondary Name Node Mapreduce JobTracker secondary ES Secondary Master node Hbase Secondary Master node	64	24	0.96	RAID 1	4 Port 10Gb
1.3		Data Node 1	1	HDFS data node Mapreduce TaskTracker ES Data node Yarn node Manager	256	48	20	RAID 5	4 Port 10Gb
1.4		Data Node 2	1	HDFS data node Mapreduce TaskTracker ES Data node Yarn node Manager	256	48	20	RAID 5	4 Port 10Gb

1.5		Data Node 3	1	HDFS data node Mapreduce TaskTracker ES Data node Yarn node Manager	256	48	20	RAID 5	4 Port 10Gb
1.6		Data Node 4	1	HDFS data node Mapreduce TaskTracker ES Data node Yarn node Manager	256	48	20	RAID 5	4 Port 10Gb
1.7		Data Node 5	1	HDFS data node Mapreduce TaskTracker ES Data node Yarn node Manager	256	48	20	RAID 5	4 Port 10Gb
2	**Máy chủ phân vùng ứng dụng (APP Zone)**		**4**						
2.1		APP	1	Apache Spark driver application HiveService Apache Drill Apache PIG Apache Mahout & SparkMlib Apache SQOOP ApacheFLUME Apache Storm Master Apache Spark cluster Manager Ambari web Tomcat	128	48	4	RAID 5	4 Port 10Gb
2.2		Worker 1	1	Kafka worker Apache Storm worker Apache Spark Worker Ambari agent	128	48	4	RAID 5	4 Port 10Gb
2.3		Worker 2	1	Kafka worker Apache Storm worker Apache Spark Worker	128	48	4	RAID 5	4 Port 10Gb

				Ambari agent					
2.4		Worker 3	1	Kafka worker Apache Storm worker Apache Spark Worker Ambari agent	128	48	4	RAID 5	4 Port 10Gb

3.2.3.4 Thiết kế chi tiết hạ tâng Bigdata

Hệ thống Bigdata được chia làm 02 phân vùng: DB Zone và App Zone

- **Phân vùng Database (DB Zone)**

Phân vùng Database quy hoạch cho toàn bộ các ứng dụng lưu trữ dữ liệu, cần đảm bảo tính bảo mật cao vì vậy cần hạn chế tối đa các truy cập trái phép hoặc không cần thiết từ các phân vùng khác, chỉ cho phép các truy cập cần thiết từ phần vùng ứng dụng và phân vùng vận hành để phục vụ vận hành hệ thống.

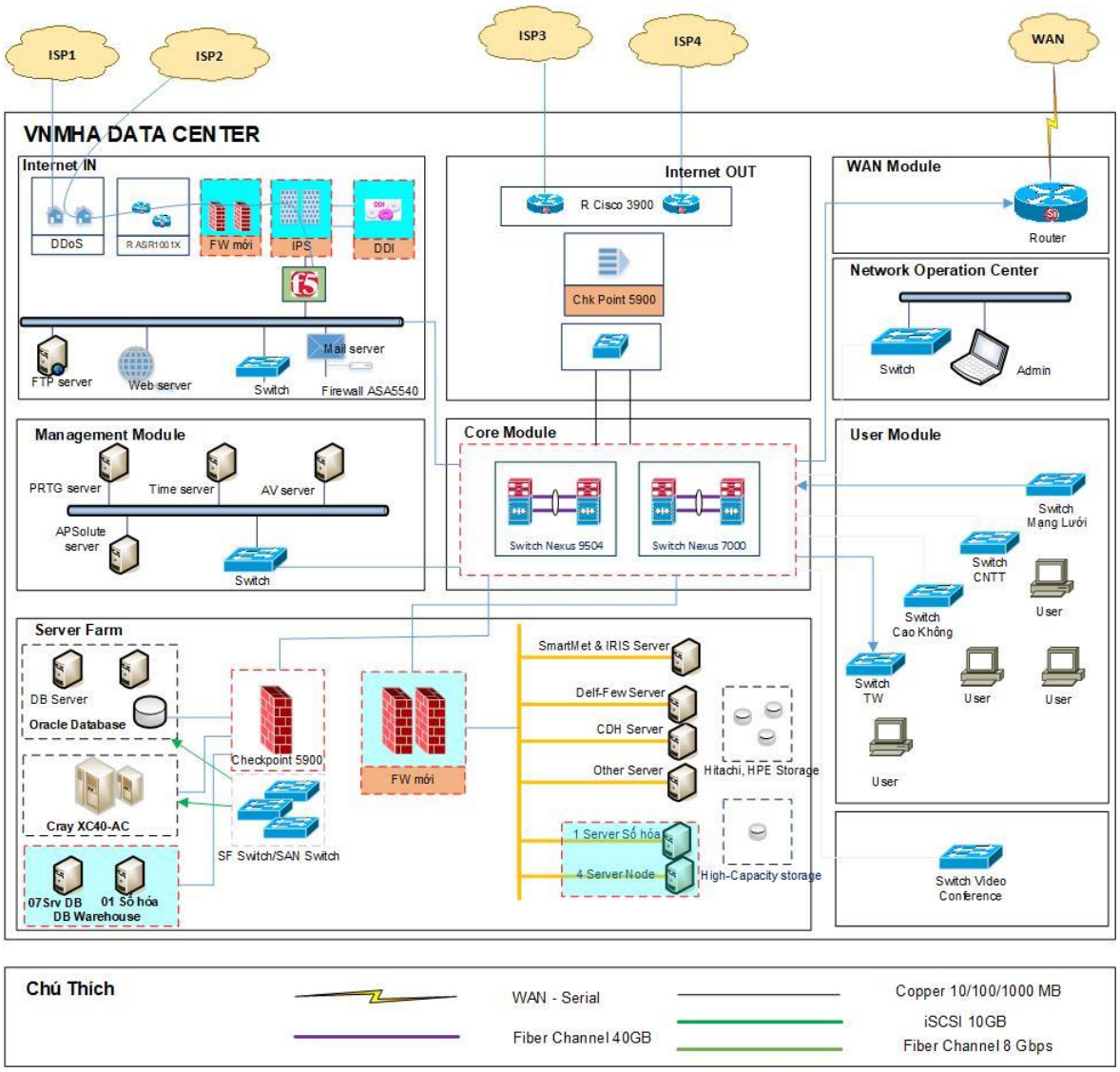
Phân vùng DB Zone bao gồm: 02 Server Name Node, 05 Server Database + 01 Server Số hóa:

- **Phân vùng ứng dụng (App Zone)**

Phần vùng ứng dụng quy hoạch cho toàn bộ các server chạy các ứng dụng cơ sở cho người dùng hoặc các ứng dụng lập trình xử lý, tính toán dữ liệu. Phân vùng này cho phép truy cập từ bên ngoài bởi người dùng, từ phân vùng VPN, phân vùng Admin để truy cập vận hành các ứng dụng.

Phân vùng App Zone bao gồm: 01 Server APP, 03 Server Worker + 01 Server Số hóa,

Như vậy, mô hình tổng thể sau khi bổ sung thiết bị cho hệ thống như sau:



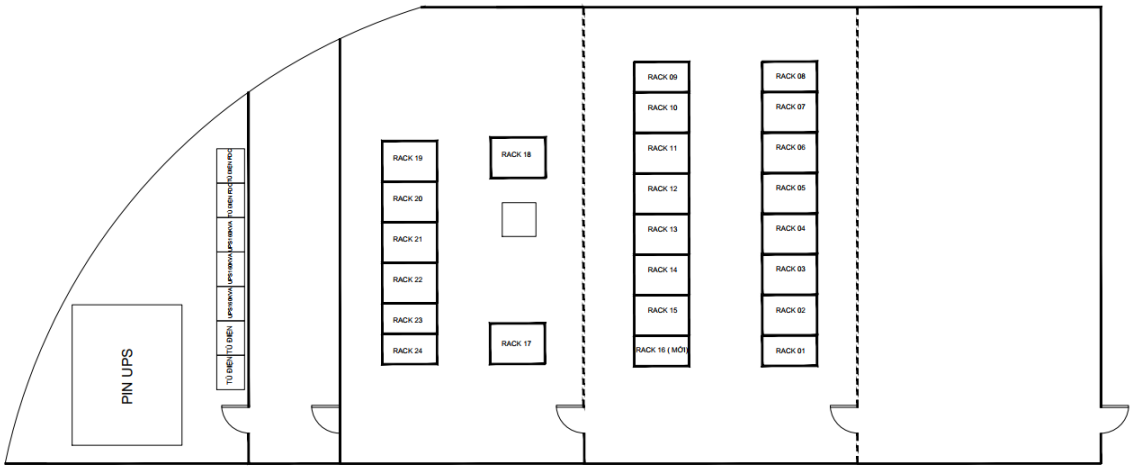
Hình 7. Mô hình tổng thể sau khi đã bổ sung thiết bị

3.2.3.5 Thông số kỹ thuật thiết bị

Thông số kỹ thuật thiết bị

STT	TÊN THIẾT BỊ	Yêu cầu kỹ thuật	ĐƠN VỊ TÍNH	SỐ LƯỢNG
I	**Trang thiết bị vận hành nền tảng CSDL hadoop và Bigdata**			
1	**Máy chủ phân vùng ứng dụng**			
1.2				**4**
	CPU	**Intel® Xeon® Gold 5318N 2.1G, 24C/48T, 11.2GT/s, 36M Cache**		2
	RAM	DDR 128GB		1
	Storage	**SSD 3x2TB (RAID 5)**		1
	Network	04x10Gbps (Bao gồm thẻ quang SFP+);		1
	Cables	04 Bộ dây nhảy quang Cable LC-LC		1
2	**Máy chủ phân vùng database**			
2.1	**Máy chủ Database Node**			**5**
	CPU	**Intel® Xeon® Gold 5318N 2.1G, 24C/48T, 11.2GT/s, 36M Cache**		2
	RAM	DDR 256GB		1
	Storage	**SSD 4x7.68TB (RAID 5)**		1
	Network	04x10Gbps (Bao gồm thẻ quang SFP+);		1
	Cables	04 Bộ dây nhảy quang Cable LC-LC		1
2.2	**Máy chủ Name Node**		**Chiếc**	**2**
	CPU	**Intel® Xeon® Silver 4410Y 2G, 12C/24T, 16GT/s, 30M Cache**		2
	RAM	DDR 64GB		1
	Storage	**SSD 02x960GB (RAID 1)**		1
	Network	04x10Gbps (Bao gồm thẻ quang SFP+);		1
	Cables	04 Bộ dây nhảy quang Cable LC-LC		1

3.2.6. Mô tả phương án lắp đặt thiết bị



MẶT BẰNG TTDL

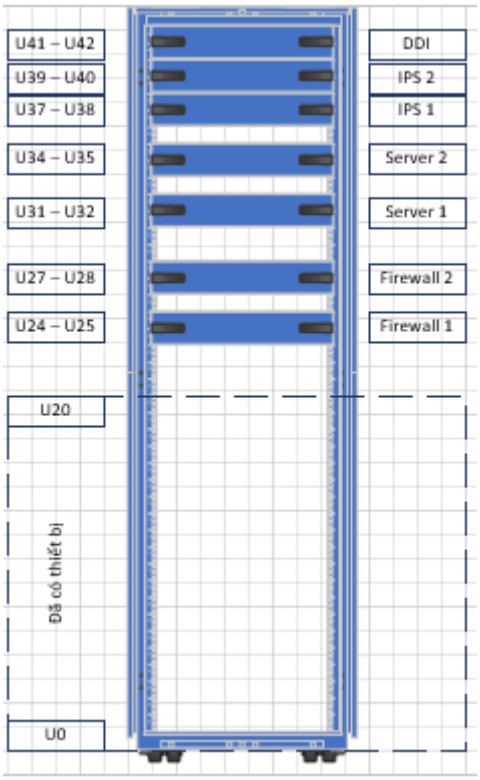
Hình 8. Sơ đồ mặt bằng Trung tâm dữ liệu

Hiện tai TTDL của Tổng cục Khí tượng Thủy văn đã đi vào hoạt động, đặt tại tầng 3, trên diện tích gần 100m2. Đã được trang bị đầy đủ tất cả các hạng mục theo tiêu chuẩn của một TTDL bao gồm: hệ thống San Nâng, UPS, báo cháy, báo khói, hệ thống điều hòa, tiếp địa…..

Hệ thống UPS: Đã được trang bị thiết bị công suất 450KVA, Công xuất tiêu thụ hiên tại chỉ chiếm 10-15%.

3.2.6.1. Phương án lắp đặt thiết bị mạng và thiết bị bảo mật

Hệ thống có bổ sung thêm 07 thiết bị, theo khảo sát tủ rack 1 tại phòng Network đang sử dụng từ U01 – U20, vì vậy, thiết bị triển khai sẽ lắp đặt tại tủ rack này.

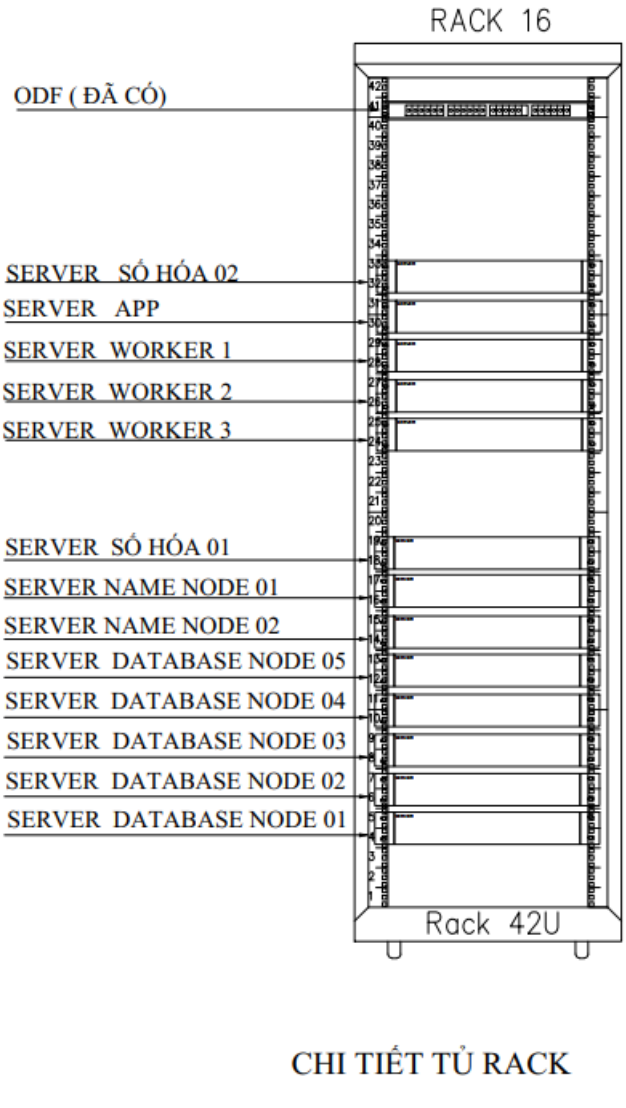


Hình 9. Sơ đồ lắp đặt thiết bị trên tủ rack

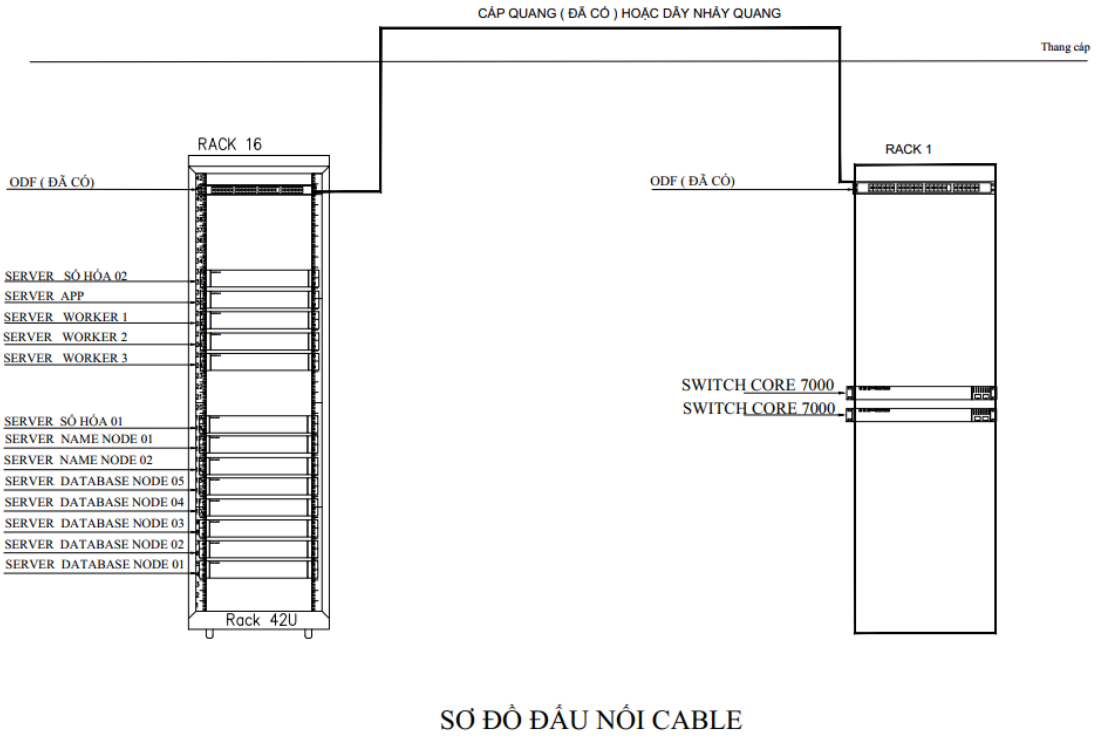
Bảng 13. Chi tiết danh sách thiết bị sẽ được lắp đặt tại tủ rack 1

TT	Thiết bị	Ghi chú	Rack1	Rack Unit (Tọa độ)
1	Firewall 1	Đầu tư mới	1	U22 – U28
2	Firewall 2	Đầu tư mới	1	
3	Switch Core 7000	Tái sử dụng	1	U30 – U34
4	Switch Core 7000	Tái sử dụng	1	
5	ATP (IDD 1000)	Đầu tư mới	1	U36 – U42
6	ATP (TPS) 1	Đầu tư mới	1	
7	ATP (TPS) 2	Đầu tư mới	1	

3.2.6.2. Phương án lắp đặt thiết bị máy chủ



Hình 10. Sơ đồ lắp đặt máy chủ trên tủ rack 16



Hình 11. Sơ đồ đấu nối cáp

- Các thiết bị Server của dự án được lắp đặt tại vị trí tủ Rack 16, đã có sẵn nguồn điện UPS cấp 02 PDU 32A.
- 07 Server database node, 04 Server node và 02 Server số hóa được kết nối với Switch core 7000 được đặt tại tủ Rack 01, bằng hệ thống cáp quang có sẵn hoặc sử dụng dây nhảy quang.

3.2.7. Đào tạo hướng dẫn sử dụng

Bao gồm 02 khóa gồm: (1) Lắp đặt và vận hành thiết bị; (2) Cài đặt và cấu hình, quản trị hệ thống, nội dung gồm:

3.2.7.1. Lắp đặt và vận hành thiết bị

Nội dung đào tạo lắp đặt và vận hành thiết bị

TT	Nội dung đào tạo	Ghi chú
1	Lắp đặt thiết bị (Bao gồm cả raiser)	Theo hướng dẫn của hãng
2	Lắp đặt thiết bị trên Tủ rack	Theo tiêu chuẩn của DC
3	Đấu nối mạng nội bộ	Theo tiêu chuẩn của DC

4	Tích hợp với hệ thống mạng Chủ đầu tư	Theo tiêu chuẩn của DC
5	Đấu nối nguồn điện	Theo tiêu chuẩn của DC
6	Tiếp đất	Theo tiêu chuẩn của DC
7	Kỹ thuật bật/tắt thiết bị	Theo hướng dẫn của nhà sản xuất
8	Quan sát đèn tín hiệu	Theo hướng dẫn của nhà sản xuất
9	Kiểm tra xác định thiết bị có cảnh báo hay không	Theo hướng dẫn của nhà sản xuất
10	Quy tắc đặt tên, đánh nhãn, dán nhãn thiết bị	Theo tiêu chuẩn của DC
11	Chuẩn đoán các tình huống hay xảy ra	

3.2.7.2. Khóa học cài đặt và cấu hình, quản trị hệ thống

Nội dung khóa học cài đặt và cấu hình, quản trị hệ thống

TT	**Nội dung đào tạo**	**Ghi chú**
1	Cài đặt và cấu hình Raid	Theo khuyến nghị của hãng
2	Cấu hình các hệ điều hành	Theo thiết kế
3	Tích hợp mạng mạng	Theo thiết kế
4	Hướng dẫn sao lưu hệ thống	Theo thiết kế
5	Hướng dẫn khôi phục hệ thống	Theo thiết kế
6	Hướng dẫn kiểm tra mạng	Kiểm tra thông mạng, mở cổng
7	Hướng dẫn kiểm tra tài nguyên hệ điều hành	CPU, Memory, HDD
8	Hướng dẫn sử dụng các công cụ giám sát	Theo khuyến nghị của hãng
9	Thực hành các tính huống hay xảy ra	

3.2.8. Đầu tư trang thiết bị chuyên dụng phục vụ lưu trữ và số hóa.

3.2.6.1 Thông số kỹ thuật chuyên dụng phục vụ lưu trữ, só hóa

1	**Máy chủ quản lý**		**Bộ**	**2**
	CPU	Intel Xeon Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache		1
	RAM	DDR 16GB		2
	HDD	03x1TB 10k RPM SAS 12Gbps (RAID 5)		1
	DVDRW	1		1
	Network	02x1Gbps		1
	Power Supply	Dual, Hot-plug, Fully Redundant Power Supply (1+1),		1
2	**Máy tính để bàn + Màn Hình**		**Bộ**	**10**
	Bộ vi xử lý - CPU	Intel core iI3 12100		1
	RAM	8GB		1
	SSD	SSD: 256 GB GB		1
	Chuột	Cổng USB		1
	Bàn phím	Cổng USB		1
	Màn hình	LED 17 inch		
3	**Máy quét khổ A0**		**Chiếc**	**1**

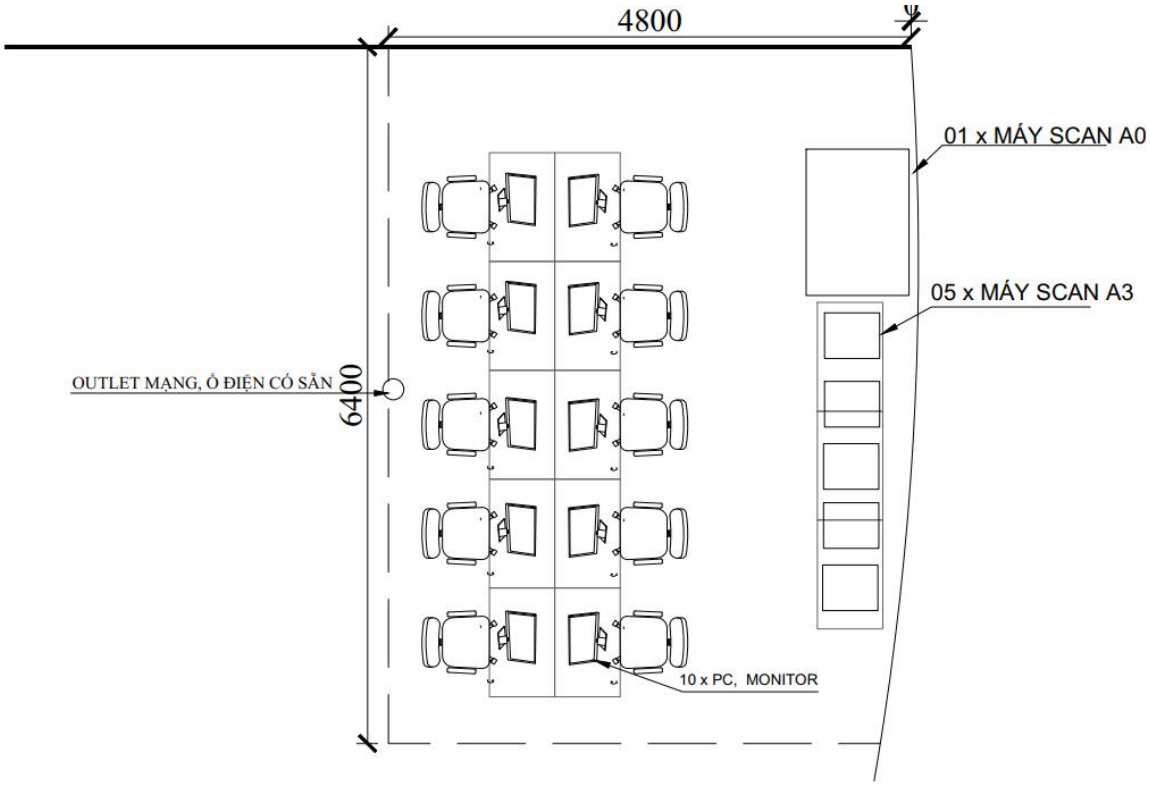
		Loại máy Scan: Máy scan khổ lớn Khổ scan tối đa: 39"/(1,001 mm) Chân máy: Có Tốc độ Scan: Trắng đen : 17m/phút - Màu : 2,75m/phút Độ phân giải: 2.400 x 1.200 dpi (tối đa 9.600 dpi) Mật độ màu: 48 bit color với scan màu Độ chính xác : +/- 0.1% Nguồn điện: 100-240 V Công suất điện: < 19 W / < 0.4 W Khối lượng (kg): 18,5 kg Kích thước (Rộng x Dài x Cao): 13,1" x47,3" x 5" Phần mềm: Rowe Scan Manager TWAIN (Tặng kèm) Scan trực tiếp tài liệu với sự hỗ trợ của TWAIN (Support) Với bộ chỉnh sửa/ điều chỉnh hình ảnh cơ bản, 2 cách xem (xem toàn cảnh và xem điểm chính) Bộ quản lý màu Icc Bảo hành 1 năm		
4	Máy quét tự động khổ A3		**Chiếc**	2
	Máy quét tự động khổ A3	Độ phân giải (dpi): 600 Kiểu quét quét 2 mặt tự động, khổ giấy A3 Tốc độ quét B/W: 80 trang/phút, 300 dpi / Màu: 30 trang/phút, 300 dpi Công suất quét/ngày: 8.000 tờ Khay giấy (ADF): 100 Phím chức năng: 4 (Up/Down/Scan/Standby) Kiểu kết nối: USB 2.0 Nguồn điện: 24 Vdc/2,7 A Kích thước (W x D x H): 436 x 262 x 266 (mm) Tương thích HĐH Windows 2000/XP/Vista/7/8 Trọng lượng (kg): 9		
7	Máy quét phẳng khổ A3		**Chiếc**	**3**

		Cảm biến hình ảnh CCD Nguồn sáng LED Độ phân giải 600dpi Công nghệ Công nghệ SEETM quét cách gáy sách 2mm Chế độ quét Màu: 48-bit đầu vào, đầu ra 24-bit Xám: 16-bit đầu vào, đầu ra 8-bit Đen trắng: 1 bit Vùng quét (WxL) Tối đa: 304.8 x 431.8 mm (12" x 17") , A3 Kiểu quét Quét sách A3 Tốc độ quét 2,48 giây/tờ (Màu, 300 dpi, A3) 2.10 giây/tờ (Xám, đen trắng, 300 dpi, A3) Công suất quét/ngày 5000 tờ Giao diện kết nối USB 2.0 Nguồn điện 24Vdc/ 1,25 A Điện năng tiêu thụ < 24W (hoạt động), <8W (chờ) Phần mềm đi kèm Plustek Book Pavilion / ABBYY FineReader 12.0 Sprint / Plustek DocTWAIN Kích thước (WxDxH) 623x400x140 mm Chuẩn kết nối Chuẩn TWAIN, WIA Tương thích HĐH Windows 7 / 8 / 10 Trọng lượng 7,7kgs		

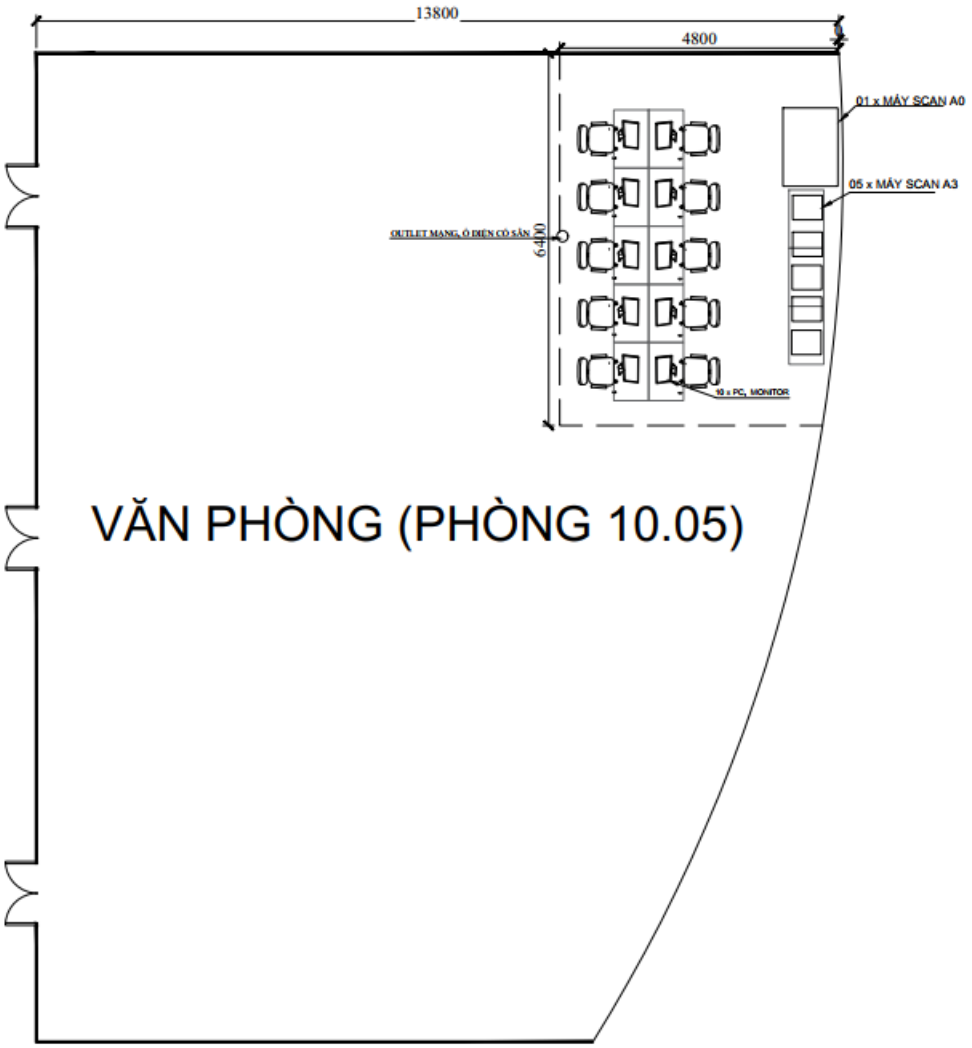
3.2.6.2 Mô tả phương án lắp đặt thiết bị số hóa

Khu vực đặt thiết bị số hóa nằm ở tầng 10, phòng 10.05 trong khu vực rộng khoảng 30m2. Với số lượng 10 bộ máy tính, 05 máy scan A3, 01 máy scan A0 hoàn toàn được bố trí phù hợp trong diện tích trên.

Phòng 10.05 đã đi vào hoạt động vì vậy nguồn điện và đầu chờ mạng đã có, hoàn toàn có thể kết nối, di chuyển dữ liệu scan lên 02 Server số hóa được lắp đặt trong TTDL.



Hình 12. Sơ đồ lắp đặt thiết bị số hóa



Hình 13. Sơ đồ lắp đặt thiết bị số hóa tại phòng 10.05

4. TỔNG DỰ TOÁN

4.1. Căn cứ lập dự toán

4.2. Nguồn vốn

4.3. Tổng mức đầu tư

4.4. Dự toán phần thiết bị bảo mật

4.5. Dự toán các dịch vụ đi kèm

4.5.1. Dự toán dịch vụ kỹ thuật cài đặt tối ưu hóa, tăng cường tính bảo mật của hệ thống CNTT hiện tại của Tổng cục KTTV

4.5.2. Dự toán dịch vụ đào tạo