Mục lục

[**I.** **Giới thiệu về Cloud computing** 2](#_Toc140601255)

[**1.** **Giới thiệu** 2](#_Toc140601256)

[**2.** **Điện toán đám mây là gì?** 2](#_Toc140601257)

[**3.** **Định nghĩa điện toán đám mây** 3](#_Toc140601258)

[**4.** **Lịch sử điện toán đám mây** 4](#_Toc140601259)

[**5.** **Các mô hình phân phối đám mây** 4](#_Toc140601260)

[**6.** **Các môi trường đám mây** 5](#_Toc140601261)

[**7.** **Lợi ích của điện toán đám mây** 6](#_Toc140601262)

[**8.** **Rủi ro, chi phí và đạo đức trong điện toán đám mây** 8](#_Toc140601263)

[**9.** **Kết luận** 10](#_Toc140601264)

[**II.** **Xây dựng mạng bằng AWS** 11](#_Toc140601265)

[**1.** **Tạo VPC** 12](#_Toc140601266)

[**2.** **Tạo Subnets public và private internet** 14](#_Toc140601267)

[**3.** **Tạo internet gateways** 17](#_Toc140601268)

[**4.** **Tạo NAT gateways** 19](#_Toc140601269)

[**5.** **Tạo route tables** 21](#_Toc140601270)

[6. **Tạo EC2 máy chủ kiểm tra truy cập của VPC** 27](#_Toc140601271)

1. **Giới thiệu về Cloud computing**

* **Giới thiệu**

Tác động của Điện toán đám mây (Cloud Computing) đối với ngành công nghiệp và người dùng cuối là rất lớn:

* Nhiều khía cạnh của cuộc sống hàng ngày đã được biến đổi bởi sự hiện diện vô cùng phổ biến của phần mềm chạy trên các mạng đám mây. Bằng cách tận dụng điện toán đám mây, các startup và doanh nghiệp có thể tối ưu hóa chi phí và tăng cường ưu đãi mà không cần mua sắm và quản lý phần cứng và phần mềm một cách riêng lẻ.
* Các nhà phát triển độc lập có quyền khởi chạy ứng dụng và dịch vụ trực tuyến có sẵn toàn cầu. Các nhà nghiên cứu có thể chia sẻ và phân tích dữ liệu ở quy mô mà trước đây chỉ dành cho các dự án được tài trợ mạnh. Và người dùng internet có thể nhanh chóng truy cập phần mềm và bộ nhớ để tạo, chia sẻ và lưu trữ phương tiện số lượng vượt xa khả năng tính toán của các thiết bị cá nhân của họ.
* **Điện toán đám mây là gì?**
* Đám mây tính toán là việc cung cấp các tài nguyên tính toán dưới dạng dịch vụ, có nghĩa là các tài nguyên này được sở hữu và quản lý bởi nhà cung cấp đám mây thay vì người dùng cuối.
* Những tài nguyên này có thể bao gồm các ứng dụng phần mềm trực tuyến (như Tik Tok hay Netflix), dịch vụ lưu trữ dữ liệu của bên thứ ba cho ảnh và phương tiện số khác (như iCloud hay Dropbox), hoặc máy chủ của bên thứ ba được sử dụng để hỗ trợ cơ sở hạ tầng tính toán của một doanh nghiệp, nghiên cứu hoặc dự án cá nhân.
* Trước sự phổ biến rộng rãi của điện toán đám mây, doanh nghiệp và người dùng máy tính chủ yếu phải mua và duy trì phần mềm và phần cứng mà họ muốn sử dụng. Với sự phát triển ngày càng có sẵn của các ứng dụng, dịch vụ, máy chủ dựa trên đám mây, doanh nghiệp và người tiêu dùng hiện có quyền truy cập vào một loạt các tài nguyên tính toán theo yêu cầu dưới dạng dịch vụ truy cập internet.
* Chuyển từ phần mềm và phần cứng trên nền tảng tại chỗ sang các tài nguyên mạng từ xa và phân tán có nghĩa là người dùng đám mây không còn phải đầu tư lao động, vốn và kiến thức cần thiết để mua và duy trì các tài nguyên tính toán này.
* Sự truy cập chưa từng có vào các tài nguyên tính toán này đã tạo ra một làn sóng mới của các doanh nghiệp dựa trên đám mây, thay đổi các thực hành công nghệ thông tin trên các ngành công nghiệp và biến đổi nhiều hoạt động hàng ngày hỗ trợ bởi máy tính. Với đám mây, cá nhân giờ đây có thể làm việc với đồng nghiệp qua các cuộc họp trực tuyến và các nền tảng cộng tác khác, truy cập nội dung giải trí và giáo dục theo yêu cầu, giao tiếp với các thiết bị gia đình, gọi xe bằng thiết bị di động và thuê phòng nghỉ trong nhà người khác.
* **Định nghĩa điện toán đám mây**
* Theo Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST), một cơ quan phi quản lý của Bộ Thương mại Hoa Kỳ với sứ mệnh thúc đẩy đổi mới, định nghĩa điện toán đám mây là:

*“Một mô hình cho phép truy cập mạng phổ biến, thuận tiện, theo yêu cầu vào một nhóm tài nguyên điện toán có thể cấu hình được được chia sẻ (ví dụ: mạng, máy chủ, lưu trữ, ứng dụng và dịch vụ) có thể được cung cấp và giải phóng nhanh chóng với nỗ lực quản lý tối thiểu hoặc tương tác với nhà cung cấp dịch vụ.”*

* NIST liệt kê năm đặc điểm thiết yếu của điện toán đám mây như sau:
* **Tự phục vụ theo yêu cầu:**

Tài nguyên đám mây có thể được truy cập hoặc cấp phát mà không cần tương tác của con người. Với mô hình này, người tiêu dùng có thể truy cập ngay lập tức vào các dịch vụ đám mây khi đăng ký. Các tổ chức cũng có thể tạo các cơ chế cho phép nhân viên, khách hàng hoặc đối tác truy cập các dịch vụ đám mây nội bộ theo yêu cầu theo logic được xác định trước mà không cần phải thông qua dịch vụ CNTT.

* **Truy cập mạng rộng rãi:**

Người dùng có thể truy cập dịch vụ và tài nguyên đám mây từ bất kỳ thiết bị nào và ở bất kỳ vị trí nào được nối mạng nếu họ có quyền.

* **Chia sẻ tài nguyên:**

Tài nguyên của nhà cung cấp đám mây được chia sẻ bởi nhiều người thuê trong khi vẫn giữ dữ liệu của khách hàng riêng biệt khỏi các khách hàng khác.

* **Độ co giãn nhanh chóng:**

Không giống như phần cứng và phần mềm tại chỗ, tài nguyên điện toán đám mây có thể được tăng, giảm hoặc sửa đổi nhanh chóng dựa trên nhu cầu thay đổi của người dùng đám mây.

* **Dịch vụ có đo lường:**

Sử dụng tài nguyên đám mây được đo lường để các doanh nghiệp và người dùng đám mây khác chỉ cần trả tiền cho các tài nguyên họ sử dụng trong bất kỳ chu kỳ thanh toán nào.

* **Lịch sử điện toán đám mây**
* Điện toán đám mây đã có các nguồn gốc từ những năm 1950 khi các trường đại học và công ty cho thuê thời gian tính toán trên máy tính mainframe. Những ý tưởng về điện toán đám mây đã được đề xuất từ những năm 1960 bởi các nhà khoa học máy tính. Tuy nhiên, điện toán đám mây không trở nên phổ biến cho đến đầu thập kỷ 21.
* Thập kỷ này chứng kiến sự ra đời của nhiều dịch vụ đám mây từ các công ty như Amazon, Google, Microsoft, IBM và DigitalOcean. Các dịch vụ này cho phép doanh nghiệp tối ưu hóa chi phí và cung cấp tài nguyên cho việc phát triển ứng dụng. Ứng dụng dựa trên đám mây (SaaS) cũng trở nên phổ biến trong thời kỳ này, cho phép người dùng truy cập ứng dụng từ nhiều thiết bị.
* Các ứng dụng dựa trên đám mây như Gmail, Google Drive, Microsoft 365, Adobe Creative Cloud, Netflix, Spotify, Dropbox, Zoom và Slack đã trở thành lựa chọn phổ biến cho doanh nghiệp và người dùng cá nhân.
* **Các mô hình phân phối đám mây**

Các nguồn lực đám mây được cung cấp theo nhiều mô hình phân phối khác nhau, cung cấp cho khách hàng các mức độ hỗ trợ và linh hoạt khác nhau.

* Infrastructure as a Service (IaaS)
* IaaS là việc cung cấp cơ sở hạ tầng điện toán theo yêu cầu, bao gồm hệ điều hành, mạng, lưu trữ và các thành phần cơ sở hạ tầng khác. Giống như một phiên bản ảo của máy chủ vật lý, IaaS giải phóng người dùng đám mây khỏi việc phải mua và bảo trì máy chủ vật lý đồng thời cũng cung cấp khả năng linh hoạt để mở rộng quy mô và trả tiền cho các tài nguyên khi cần.
* IaaS là một lựa chọn phổ biến cho các doanh nghiệp muốn tận dụng các lợi thế của đám mây và có các quản trị viên hệ thống có thể giám sát việc cài đặt, cấu hình và quản lý hệ điều hành, công cụ phát triển và các cơ sở hạ tầng cơ bản khác mà họ muốn sử dụng.
* Tuy nhiên, IaaS cũng được sử dụng bởi các nhà phát triển, nhà nghiên cứu và những người khác muốn tùy chỉnh cơ sở hạ tầng cơ bản của môi trường điện toán của họ. Do tính linh hoạt của nó, IaaS có thể hỗ trợ mọi thứ từ cơ sở hạ tầng điện toán của một công ty đến lưu trữ web đến phân tích dữ liệu lớn.
* Platform as a Service (PaaS)
* PaaS cung cấp một nền tảng điện toán nơi cơ sở hạ tầng cơ bản (như hệ điều hành và phần mềm khác) được cài đặt, cấu hình và bảo trì bởi nhà cung cấp, cho phép người dùng tập trung nỗ lực vào việc phát triển và triển khai ứng dụng trong một môi trường được kiểm tra và tiêu chuẩn hóa.
* PaaS thường được sử dụng bởi các nhà phát triển phần mềm và nhóm phát triển vì nó giảm thiểu sự phức tạp của việc thiết lập và bảo trì cơ sở hạ tầng máy tính, đồng thời cũng hỗ trợ cộng tác giữa các nhóm phân tán.
* PaaS có thể là một lựa chọn tốt cho các nhà phát triển không cần tùy chỉnh cơ sở hạ tầng cơ bản của họ, hoặc những người muốn tập trung sự chú ý vào phát triển thay vì DevOps và quản trị hệ thống.
* Software as a Service (SaaS)

Các nhà cung cấp SaaS là các ứng dụng dựa trên đám mây mà người dùng truy cập theo yêu cầu từ internet mà không cần phải cài đặt hoặc bảo trì phần mềm. Ví dụ bao gồm GitHub, Google Docs, Slack và Adobe Creative Cloud. Ứng dụng SaaS rất phổ biến đối với doanh nghiệp và người dùng chung vì chúng thường dễ sử dụng, có thể truy cập từ bất kỳ thiết bị nào và có các phiên bản miễn phí, cao cấp và doanh nghiệp của ứng dụng. Giống như PaaS, SaaS loại bỏ cơ sở hạ tầng cơ bản của ứng dụng phần mềm để người dùng chỉ được tiếp xúc với giao diện mà họ tương tác.

* **Các môi trường đám mây**

Các dịch vụ đám mây có sẵn dưới dạng tài nguyên công cộng hoặc riêng tư, mỗi loại phục vụ các nhu cầu khác nhau.

* Môi trường đám mây công cộng (Public Cloud):
* Môi trường đám mây công cộng đề cập đến các dịch vụ đám mây (như máy ảo, lưu trữ hoặc ứng dụng) được cung cấp công khai bởi nhà cung cấp thương mại cho doanh nghiệp và cá nhân.
* Tài nguyên đám mây công cộng được lưu trữ trên phần cứng của nhà cung cấp thương mại, người dùng truy cập qua internet. Chúng không phải lúc nào cũng phù hợp với các tổ chức trong các ngành có quy định cao, chẳng hạn như chăm sóc sức khỏe hoặc tài chính, vì môi trường đám mây công cộng có thể không tuân thủ các quy định của ngành về dữ liệu khách hàng.
* Môi trường đám mây riêng (Private Cloud):
* Môi trường đám mây riêng đề cập đến các dịch vụ đám mây được sở hữu và quản lý bởi tổ chức sử dụng chúng và chỉ dành cho nhân viên và khách hàng của tổ chức.
* Môi trường đám mây riêng cho phép các tổ chức kiểm soát nhiều hơn đối với môi trường điện toán và dữ liệu được lưu trữ của họ, điều này có thể cần thiết cho các tổ chức trong các ngành có quy định cao.
* Môi trường đám mây riêng đôi khi được coi là an toàn hơn đám mây công cộng vì chúng được truy cập qua mạng riêng và cho phép tổ chức giám sát trực tiếp bảo mật đám mây của họ. Các nhà cung cấp đám mây công cộng đôi khi cung cấp dịch vụ của họ dưới dạng ứng dụng có thể được cài đặt trên môi trường đám mây riêng, cho phép các tổ chức giữ cơ sở hạ tầng và dữ liệu của họ tại chỗ trong khi vẫn tận dụng các đổi mới mới nhất của đám mây công cộng.
* Môi trường đám mây lai và đa đám mây (Hybrid Cloud and Multicloud):

Nhiều tổ chức sử dụng môi trường đám mây lai kết hợp tài nguyên đám mây công cộng và riêng tư để hỗ trợ nhu cầu điện toán của tổ chức trong khi vẫn duy trì tuân thủ quy định của ngành. Môi trường đám mây đa đám mây cũng phổ biến, bao gồm việc sử dụng nhiều nhà cung cấp đám mây công cộng (ví dụ: kết hợp Amazon Web Services và DigitalOcean).

* **Lợi ích của điện toán đám mây**

Điện toán đám mây mang lại nhiều lợi ích cho cá nhân, doanh nghiệp, nhà phát triển và các tổ chức khác. Những lợi ích này khác nhau tùy theo mục tiêu và hoạt động của người dùng đám mây.

* Đối với doanh nghiệp và ngành công nghiệp:
* Trước khi điện toán đám mây trở nên phổ biến, hầu hết các doanh nghiệp và tổ chức cần mua và bảo trì phần mềm và phần cứng hỗ trợ hoạt động điện toán của họ. Khi các tài nguyên điện toán đám mây trở nên khả dụng, nhiều doanh nghiệp bắt đầu sử dụng chúng để lưu trữ dữ liệu, cung cấp phần mềm doanh nghiệp và triển khai các sản phẩm và dịch vụ trực tuyến. Một số trong những áp dụng và đổi mới dựa trên đám mây này là ngành cụ thể.
* Trong lĩnh vực chăm sóc sức khỏe, nhiều nhà cung cấp sử dụng các dịch vụ đám mây được thiết kế specifically để lưu trữ và chia sẻ dữ liệu bệnh nhân hoặc giao tiếp với bệnh nhân.
* Trong học thuật, giáo viên và nhà nghiên cứu sử dụng các ứng dụng giảng dạy và nghiên cứu dựa trên đám mây.
* Nhưng cũng có một số lượng lớn các công cụ dựa trên đám mây chung đã được áp dụng trên các ngành, chẳng hạn như ứng dụng cho năng suất, nhắn tin, quản lý chi phí, hội nghị video, quản lý dự án, bản tin, khảo sát, quản lý quan hệ khách hàng, quản lý danh tính và lịch trình.
* Sự phát triển nhanh chóng của các ứng dụng và cơ sở hạ tầng kinh doanh dựa trên đám mây cho thấy đám mây không chỉ thay đổi chiến lược CNTT của doanh nghiệp: nó còn là một doanh nghiệp đang bùng nổ.
* Các công nghệ dựa trên đám mây mang lại cho các doanh nghiệp một số lợi thế chính. Đầu tiên, chúng có thể giúp tối ưu hóa chi phí CNTT. Khi các doanh nghiệp chuyển sang thuê tài nguyên điện toán, họ không còn phải đầu tư nhiều vào việc mua và bảo trì cơ sở hạ tầng CNTT tại chỗ.
* Điện toán đám mây cũng rất linh hoạt, cho phép các doanh nghiệp mở rộng quy mô (và chỉ trả tiền cho) các tài nguyên điện toán họ thực sự sử dụng. Chi phí không phải là yếu tố duy nhất thúc đẩy việc áp dụng đám mây trong kinh doanh. Các công nghệ dựa trên đám mây có thể giúp làm cho các quy trình CNTT nội bộ hiệu quả hơn khi chúng có thể được truy cập theo yêu cầu bởi nhân viên mà không cần phải thông qua các quy trình phê duyệt CNTT. Các ứng dụng dựa trên đám mây có thể cải thiện sự cộng tác trong một doanh nghiệp vì chúng cho phép giao tiếp và chia sẻ dữ liệu theo thời gian thực.
* Đối với nhà phát triển độc lập
* Các tài nguyên điện toán mà trước đây chỉ có thể mua được với chi phí cao cho các công ty lớn và tổ chức hiện nay có sẵn theo yêu cầu thông qua kết nối internet và với một phần nhỏ chi phí trước đây của chúng. Theo nghĩa đó, các nhà phát triển độc lập có thể triển khai và thử nghiệm ứng dụng dựa trên đám mây một cách nhanh chóng.
* Các ứng dụng dựa trên đám mây để chia sẻ mã (như GitHub) cũng đã giúp các nhà phát triển dễ dàng hơn trong việc xây dựng và cộng tác trên các dự án phần mềm mã nguồn mở. Ngoài ra, các nền tảng giáo dục dựa trên đám mây và các bài hướng dẫn mã hóa tương tác đã mở rộng quyền truy cập vào giáo dục nhà phát triển, cho phép những người không có đào tạo kỹ thuật chính thức học cách viết mã trong thời gian của họ.
* Nhìn chung, các nguồn lực điện toán và giáo dục dựa trên đám mây này đã giúp giảm bớt các rào cản đối với việc học các kỹ năng nhà phát triển và triển khai ứng dụng dựa trên đám mây. Đào tạo chính thức, hỗ trợ của công ty và số lượng vốn khởi nghiệp lớn không còn cần thiết để cá nhân có thể thử nghiệm tạo và triển khai ứng dụng, cho phép nhiều cá nhân tham gia vào phát triển đám mây, cạnh tranh với các công ty trong ngành và tạo và chia sẻ ứng dụng như các dự án phụ.
* Đối với các nhà nghiên cứu:

Khi các phương pháp học máy trở nên ngày càng quan trọng trong nghiên cứu khoa học, điện toán đám mây đã trở thành điều cần thiết cho nhiều lĩnh vực khoa học, bao gồm thiên văn học, vật lý, genomics và trí tuệ nhân tạo. Khối lượng dữ liệu khổng lồ được thu thập và phân tích trong các dự án nghiên cứu học máy và dữ liệu khác thường yêu cầu tài nguyên điện toán vượt quá khả năng của phần cứng.

* **Rủi ro, chi phí và đạo đức trong điện toán đám mây**

Mặc dù đám mây mang lại nhiều lợi ích, nhưng nó cũng đi kèm với một số rủi ro, chi phí và các câu hỏi về đạo đức cần được xem xét. Một số vấn đề này có liên quan đến tất cả người dùng đám mây, trong khi những vấn đề khác áp dụng nhiều hơn cho các doanh nghiệp và tổ chức sử dụng đám mây để lưu trữ dữ liệu của khách hàng:

Các cân nhắc dành cho tất cả người dùng đám mây:

* **Bảo mật:** Tài nguyên đám mây có thể có các lỗ hổng bảo mật bổ sung (so với các trung tâm dữ liệu tại chỗ truyền thống) do việc sử dụng API, thông tin đăng nhập dựa trên đám mây và các dịch vụ theo yêu cầu khiến cho việc kẻ tấn công có được quyền truy cập trái phép dễ dàng hơn. Tìm hiểu các biện pháp mà nhà cung cấp dịch vụ đám mây thực hiện để bảo vệ dữ liệu khách hàng khỏi bị đánh cắp và các cuộc tấn công khác và các thực tiễn hoặc dịch vụ bổ sung mà khách hàng có thể triển khai để bảo vệ dữ liệu của họ.
* **Mất dữ liệu:** Cũng giống như các thiết bị được sở hữu hoặc quản lý vật lý, các dịch vụ đám mây có thể bị mất dữ liệu được lưu trữ vĩnh viễn do thảm họa vật lý, lỗi, đồng bộ hóa không mong muốn, lỗi do người dùng tạo ra hoặc các vấn đề không lường trước được. Khi triển khai dịch vụ đám mây, hãy tìm hiểu các dịch vụ sao lưu mà nhà cung cấp cung cấp và lưu ý rằng chúng có thể không được cung cấp tự động hoặc miễn phí. Bạn cũng có thể chọn tự chạy sao lưu.
* **Tính bền vững của dữ liệu:** Có những lúc người dùng đám mây có thể muốn đảm bảo việc xóa dữ liệu cá nhân họ đã cung cấp cho nhà cung cấp dịch vụ đám mây. Tuy nhiên, các quy trình xóa dữ liệu trên tài nguyên đám mây và xác minh việc xóa có thể mất thời gian, phức tạp hoặc thậm chí là không thể. Trước khi cho nhà cung cấp đám mây truy cập vào dữ liệu của bạn, hãy tìm hiểu chính sách của họ về việc xóa dữ liệu trong trường hợp bạn muốn xóa dữ liệu sau này.
* **Chi phí:** Mặc dù đám mây có thể cung cấp các dịch vụ điện toán với chi phí bằng một phần nhỏ so với chi phí sở hữu chúng, nhưng chi phí cho các dịch vụ đám mây có thể nhanh chóng tăng lên khi sử dụng. Khi đăng ký dịch vụ đám mây, hãy kiểm tra chi tiết thanh toán để tìm hiểu cách thức tính phí dịch vụ và bạn có thể đặt giới hạn hoặc thông báo khi sử dụng vượt quá giới hạn mong muốn của mình hay không. Cũng đáng để tìm hiểu cách thức thông báo chi tiết thanh toán, vì phương thức thanh toán của một số nhà cung cấp không phải lúc nào cũng dễ hiểu.
* **Mất khả năng chuyển đổi nhà cung cấp:** Người dùng dịch vụ đám mây độc quyền có thể có nhiều nguy cơ bị khóa nhà cung cấp, hoặc tình trạng mà việc thay đổi nhà cung cấp trở nên khó khăn hoặc không thể thực hiện được sau khi các hoạt động tính toán được cấu trúc để phù hợp với hệ thống độc quyền, khép kín. Sử dụng các giải pháp đám mây mã nguồn mở có thể giúp giảm thiểu rủi ro này vì các tiêu chuẩn mở của nó giúp dễ dàng di chuyển các hoạt động tính toán từ nhà cung cấp này sang nhà cung cấp khác. Tuy nhiên, người dùng đám mây nên lưu ý rằng bất kỳ quá trình di chuyển nào cũng sẽ cần có công việc, kế hoạch và chuyên môn.
* **Việc sử dụng dữ liệu của công ty:** Các nhà cung cấp dịch vụ đám mây có thể sử dụng dữ liệu để hiểu cách khách hàng sử dụng sản phẩm của họ, bán hoặc cá nhân hóa quảng cáo, đào tạo thuật toán học máy hoặc thậm chí bán dữ liệu khách hàng cho các bên ngoài. Nếu bạn có lo ngại về cách dữ liệu của bạn hoặc tổ chức của bạn được sử dụng, hãy đảm bảo tìm hiểu các chính sách của nhà cung cấp dịch vụ về việc sử dụng dữ liệu đó.
* **Đạo đức của công ty:** Do sức mạnh to lớn mà một số nhà cung cấp dịch vụ đám mây có đối với thế giới, người dùng đám mây có thể muốn xem xét đạo đức của công ty mà họ đang hỗ trợ. Việc xem xét thực tiễn của công ty về các vấn đề như thu thập dữ liệu, quảng cáo, ngôn luận thù hận
* **Kết luận**

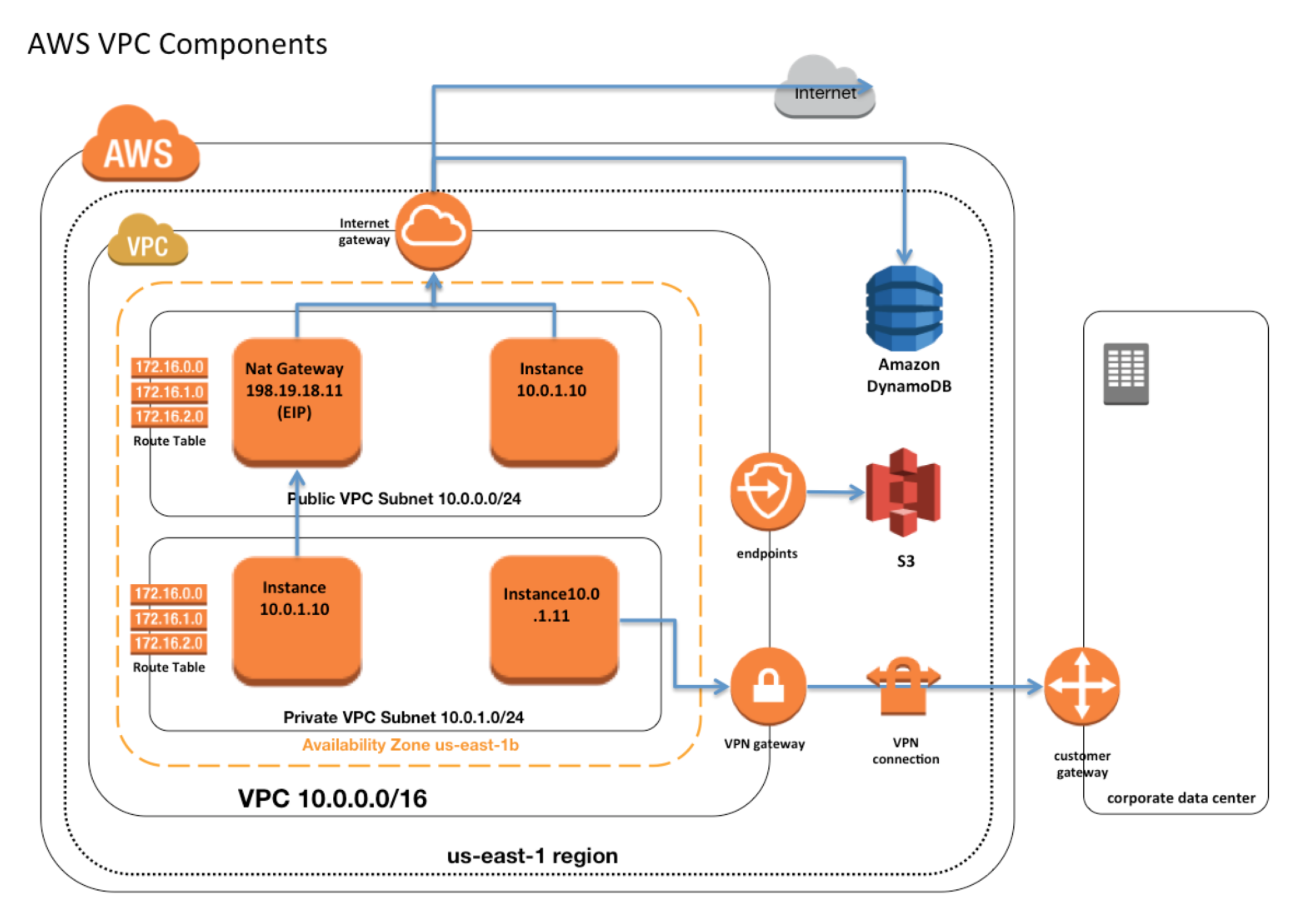
Các công nghệ đám mây mang lại nhiều cơ hội cho các doanh nghiệp, nhà phát triển độc lập, nhà nghiên cứu, nhà giáo dục và sinh viên. Bằng cách hiểu các dịch vụ, mô hình, lợi ích và rủi ro khác nhau được cung cấp bởi đám mây, người dùng có thể đưa ra quyết định sáng suốt về cách tận dụng tối đa các dịch vụ của đám mây.

Nhìn chung, đám mây là một công nghệ quan trọng có thể mang lại nhiều lợi ích cho người dùng. Tuy nhiên, cũng cần cân nhắc các rủi ro, chi phí và các vấn đề về đạo đức liên quan trước khi quyết định triển khai đám mây.

1. **Xây dựng mạng bằng AWS**

**Mạng nội bộ** là một không gian các thiết bị được kết nối với nhau qua LAN (dây mạng) hoặc Wifi (không dây) cho phép chia sẻ dữ liệu qua lại của các thiết bị với nhau, có thể là máy tính với máy tính, máy tính với camera,… nhằm bảo mật những thông tin, tài liệu chỉ được phép lưu hành trong công ty, tổ chức.

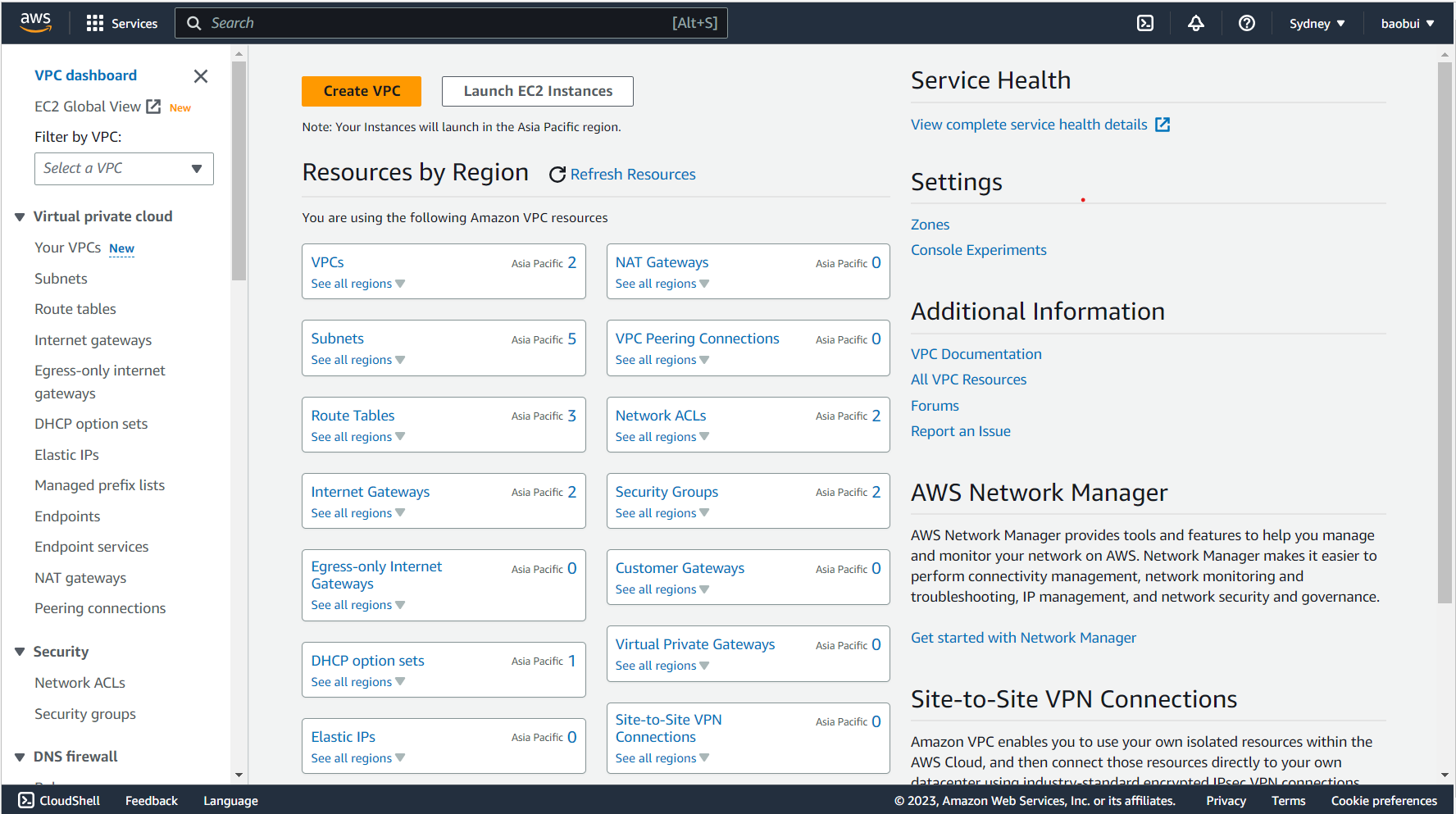
Tương tự vậy, mạng nội bộ trên AWS cloud (VPC) chính xác là những đặc tính của mạng nội bộ. Nhưng không cần cài đặt dây mạng lằng nhằng, không mất diện tích đặt phần cứng, và tính liên tục lên cao, lợi ích hơn cả là cả thiện hiệu xuất giúp mọi thứ hoạt động trơn tru hơn cũng như tính bảo mật cao và rất nhiều lợi ích khác mà các nhà dịch vụ đám mây cung cấp.

**Các thành phần của một VPC**

* Các bước tạo một VPC:
* Bước 1: Tạo VPC
* Bước 2: Tạo Subnets public và private internet
* Bước 3: Tạo internet gateways
* Bước 4: Tạo route tables
* Bước 5: Tạo NAT gateways
* Bước 6: Tạo EC2 máy chủ kiểm tra truy cập của VPC.

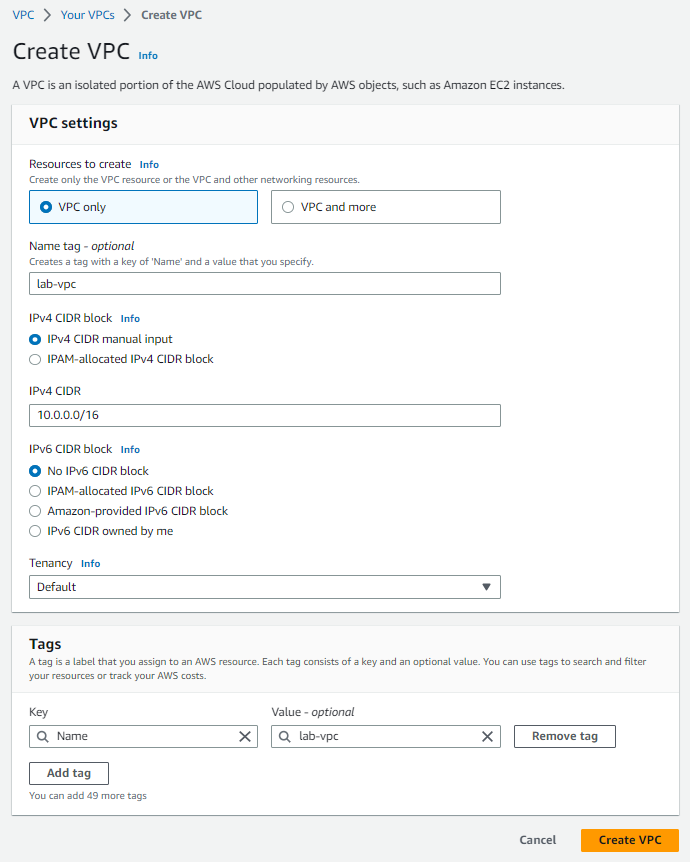
1. **Tạo VPC**

Truy cập [VPC Management Console](https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-northeast-1#Home:) và nhấn **Create VPC**

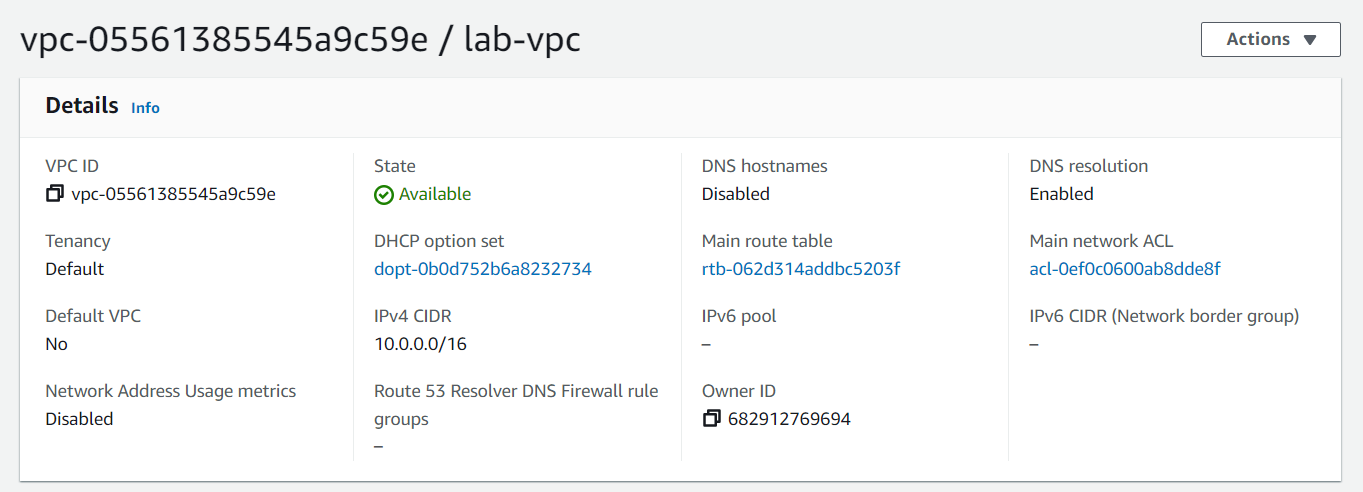
****

* Thiết lập các cài đặt:
  + **Resource to create:** VPC only
  + **Name tag:** Tên của Công ty/dự án (ở đây để là lab-vpc)
  + **IPv4 CIDR block:** Có thể hiểu là cấu hình lớp mạng (lớp mạng gồm có lớp A B C) tương đương với nó mỗi loại lớp mạng sẽ có vùng số lượng IP khác (ở đây dùng mạng lớp A để định nghĩa.)
  + **IPv6 CIDR block:** Sử dụng IPv6 (ở đây không dùng)
  + **Tenancy:** Được hiểu đơn giản là lựa chọn một hệ thống ảo hóa riêng (ở đây để default)

Nhấn **Create VPC**

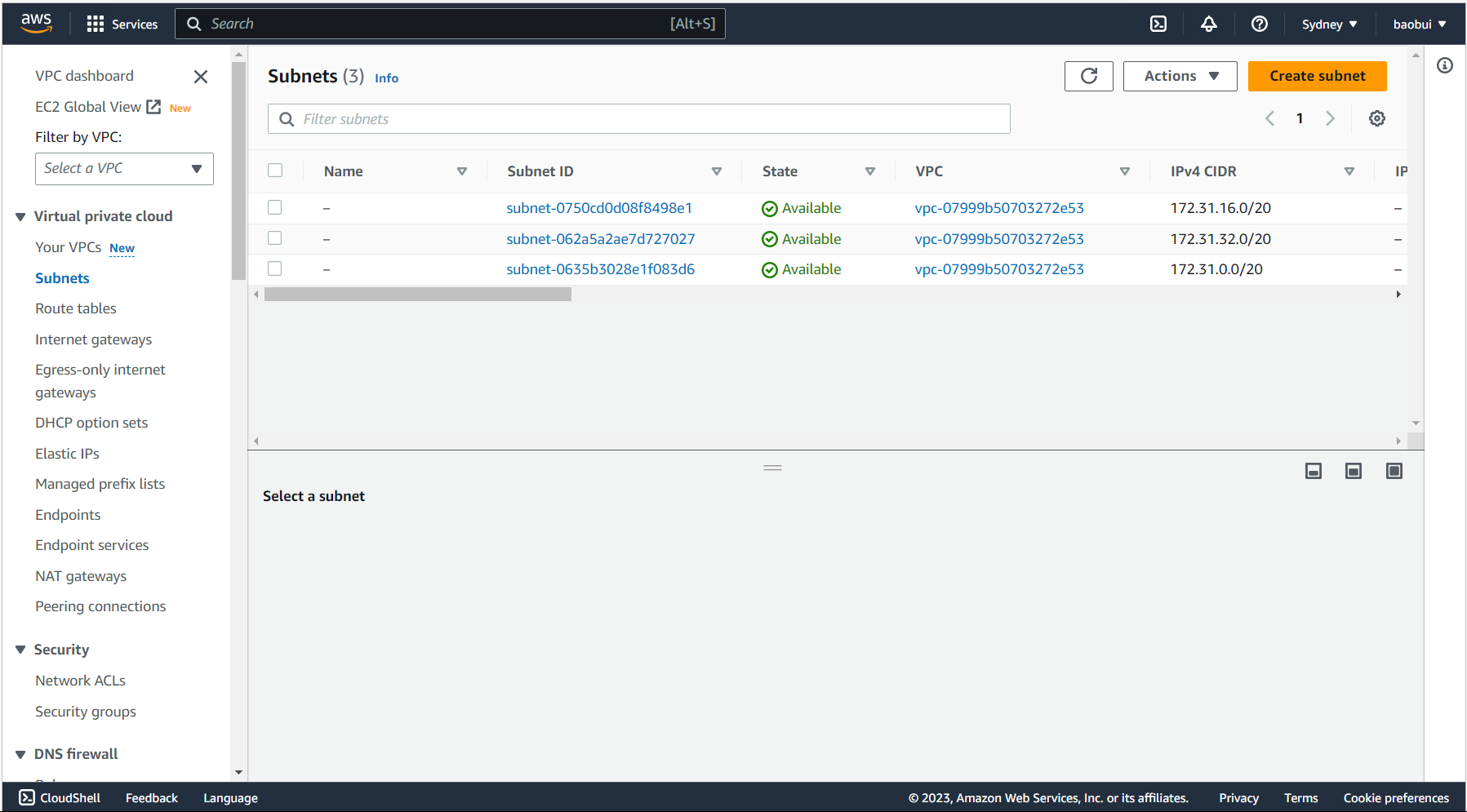
****

**Tạo thành công - thông tin/trạng thái của VPC**

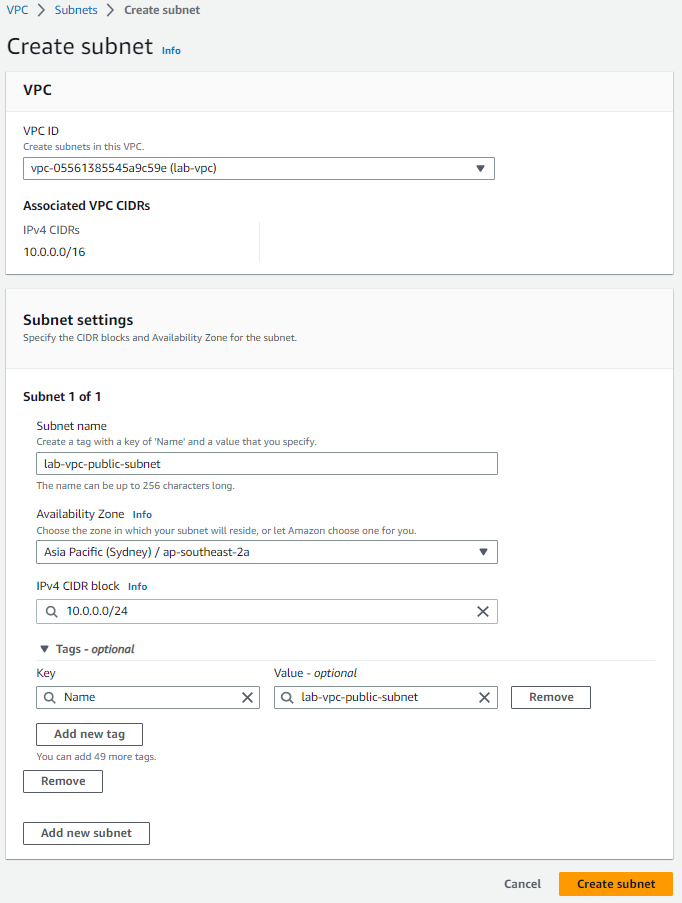
****

1. **Tạo Subnets public và private internet**

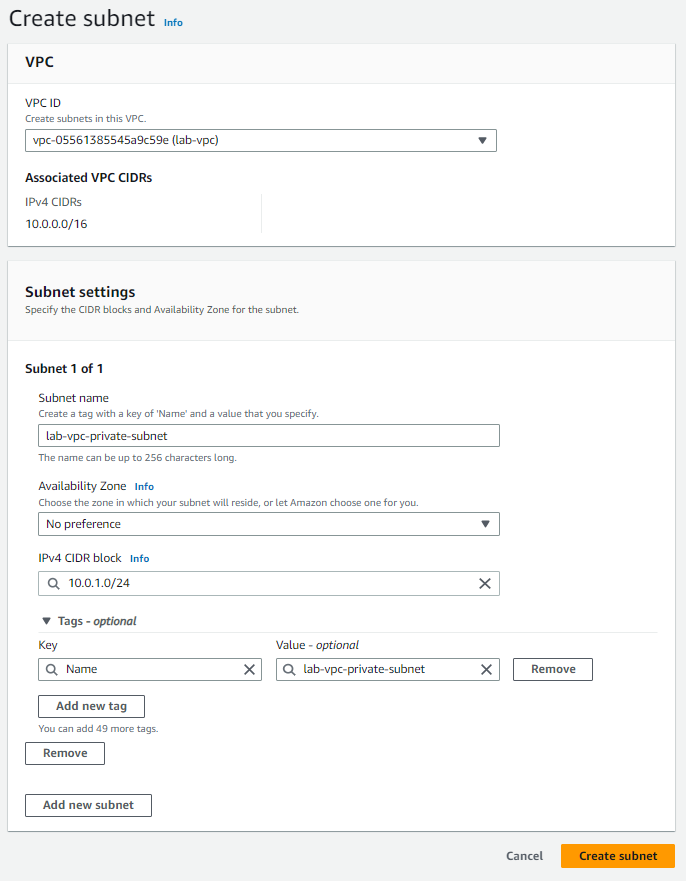
Truy cập [Subnets | VPC Management Console](https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-northeast-1#subnets:) và nhấn **Create subnet**

****

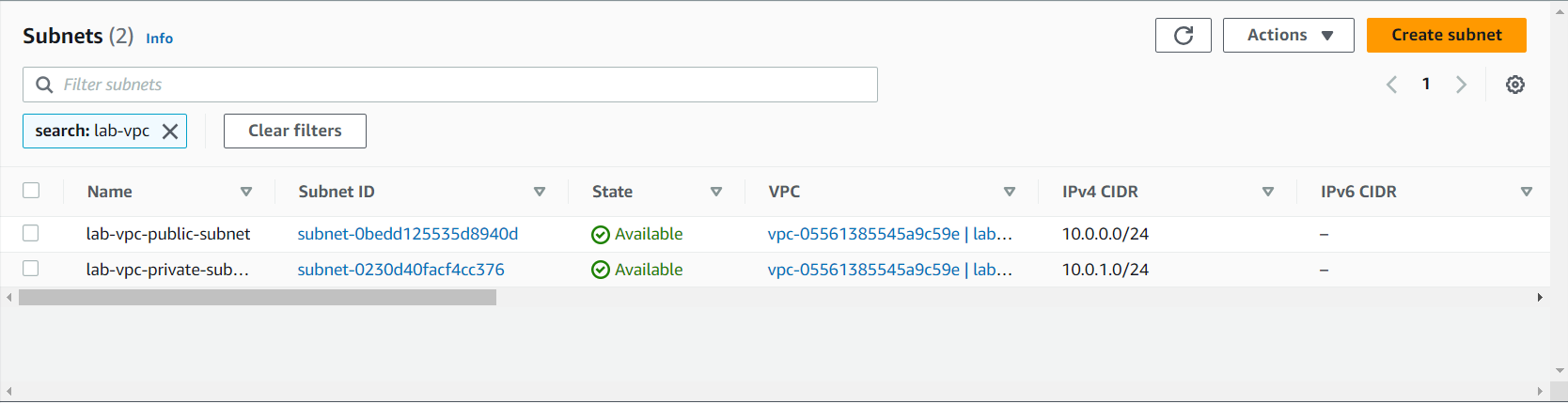
* Thiết lập các cài đặt:
  + Ở Region hiện tại (Sydney) có 3 Subnet tương ứng là ap-northeast-2a, ap-northeast-2 , ap-northeast-2c (ở đây chỉ dùng 2 subnet để tạo 1 public subnet và 1 private subnet)
  + **VPC ID:** Chọn VPC vừa tạo
  + **Subnet 1 of 1:**
    - Subnet name: lab-vpc-public-subnet
    - Availability Zone: ap-northeast-2a
  + **IPv4 CIDR block:** 10.0.0.0/24
* Nhấn **Create subnet**



Tương tự như vậy tiến hành tạo private Subnet tiếp theo với **Availability Zone**: **ap-northeast-2b**

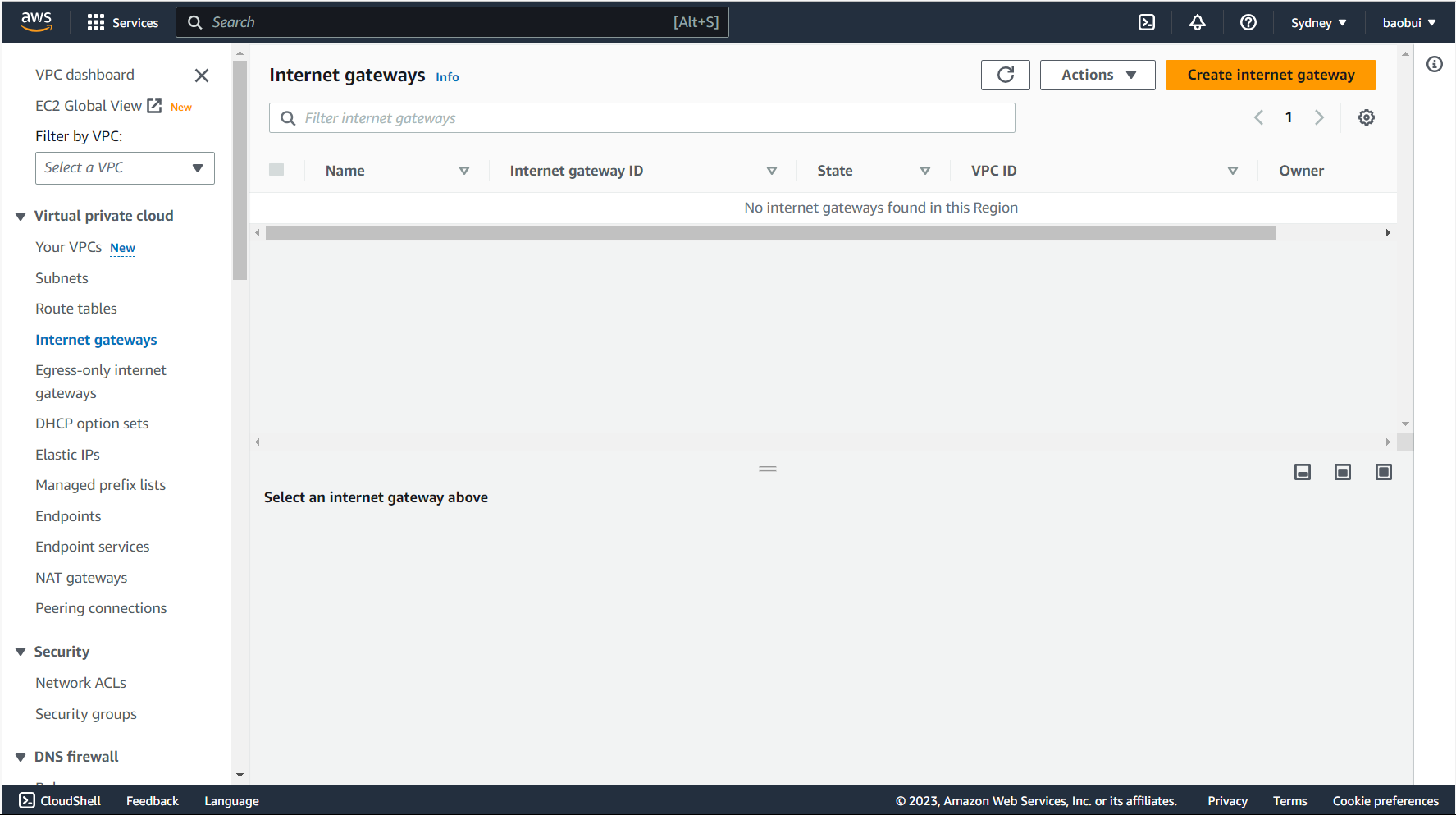


Vậy là chúng ta đã có 2 subnet

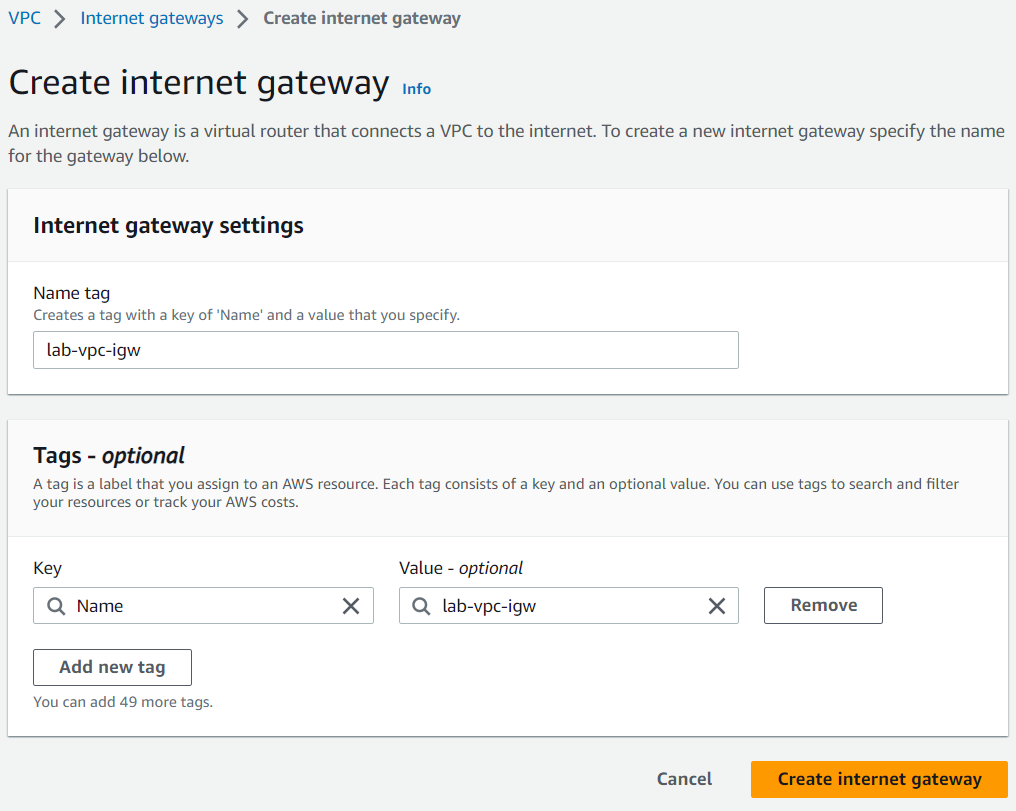


1. **Tạo internet gateways**

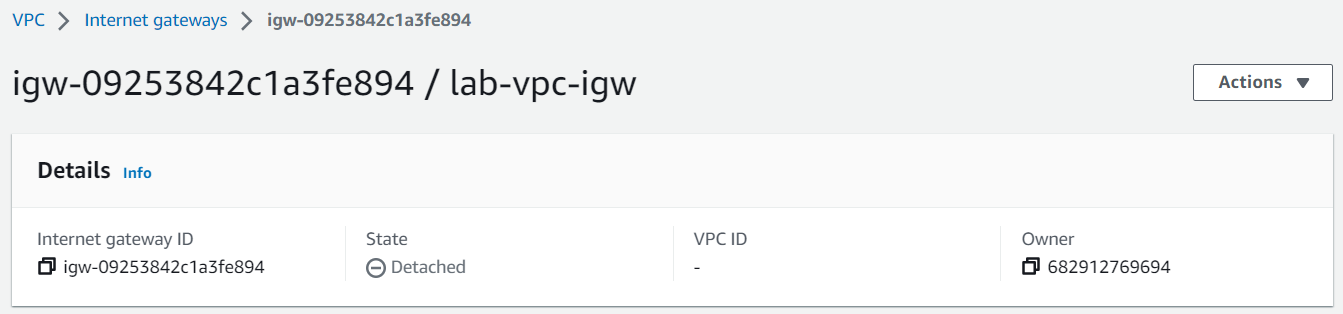
Truy cập [Internet gateways | VPC Management Console](https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-northeast-1#igws:) và nhấn **Create internet gateway**

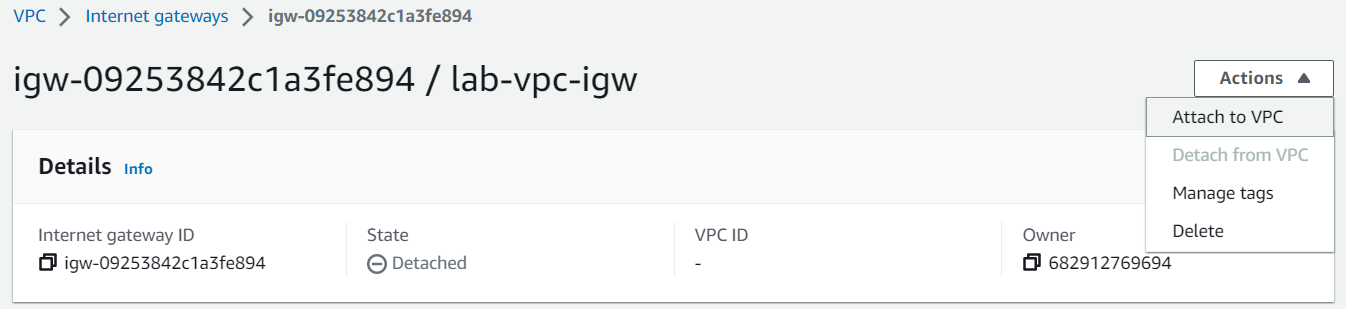
****

Điền tên Internet gateway phù hợp(ở đây là lab-vpc-igw) và nhấn **Create internet gateway**

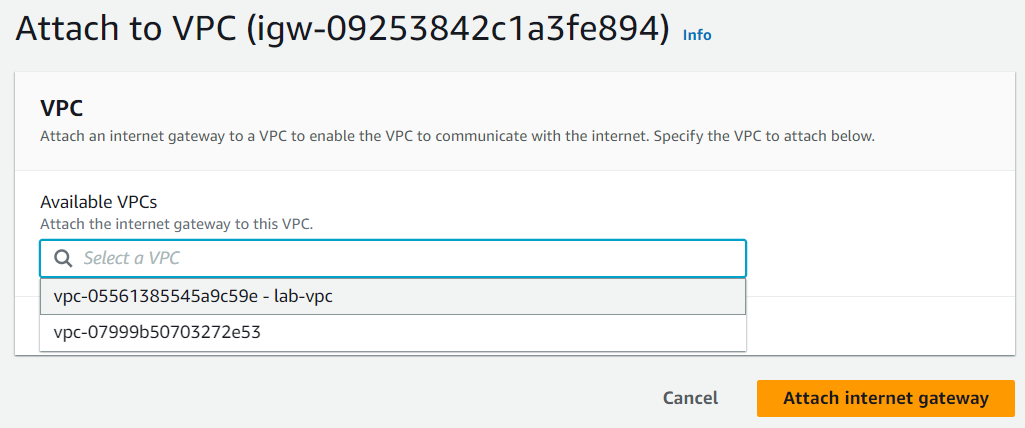
****

Đã tạo thành công internet gateway nhưng hiện tại trạng thái là **Detached** tức chưa được Attach vào VPC nào (cánh cổng chưa được gắn với intance VPC và internet).

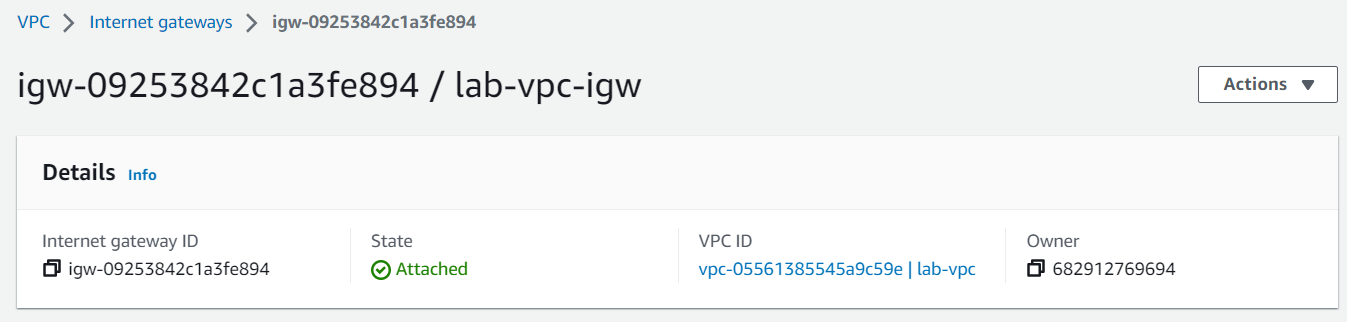
****Tiến hành chọn vào **Action** và chọn **Attach to VPC**

****

Tiến hành chọn VPC của chúng ta và nhấn **Attach internet gateway**

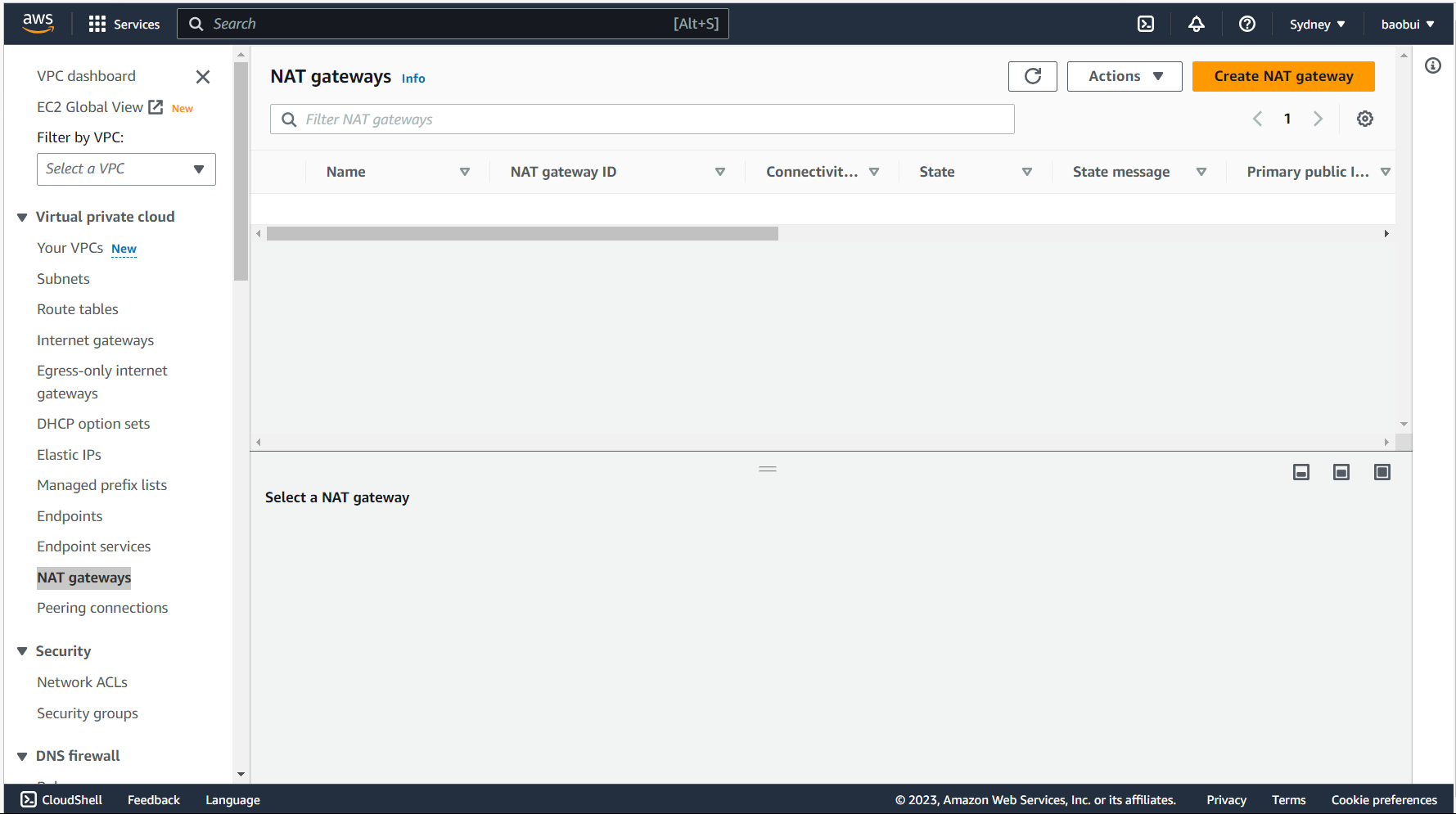
****

Trạng thái đã được **Attached** là thành công

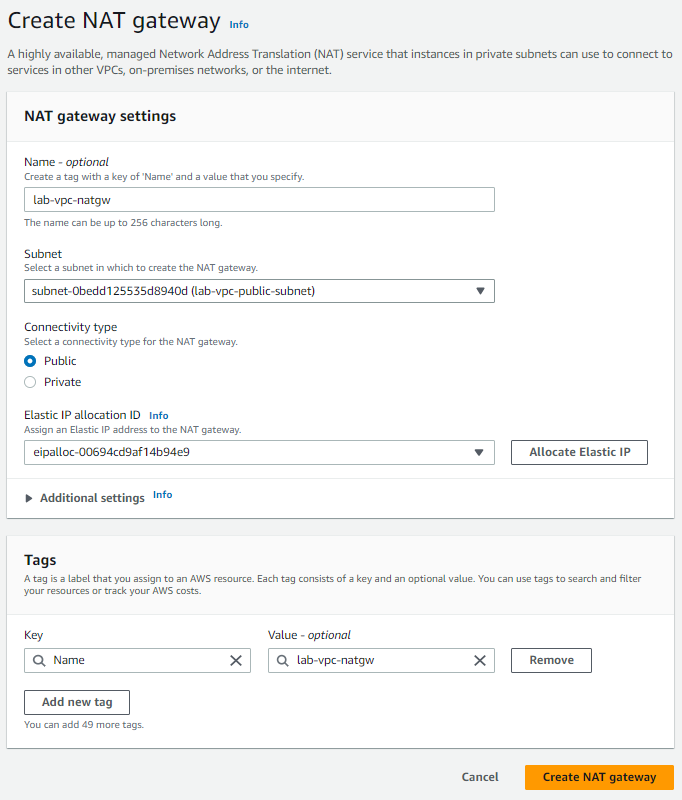
****

1. **Tạo NAT gateways**

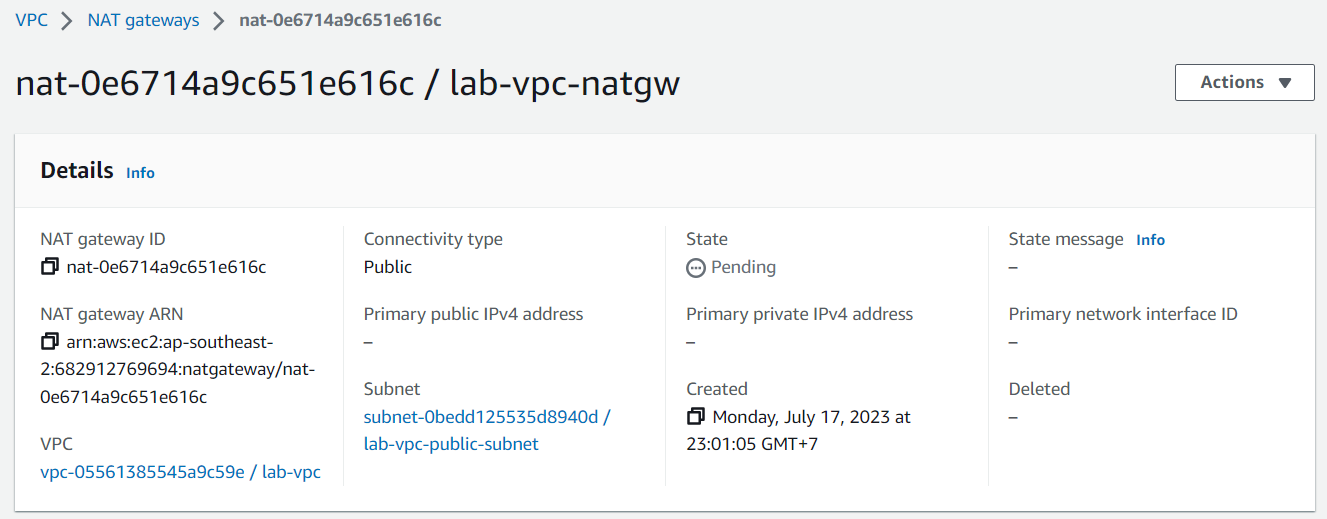
Truy cập [NAT gateways](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#NatGateways:) và nhấn **Create NAT gateway**



* Thiết lập các cài đặt:
  + **Name:** lab-vpc-natgw
  + **Subnet:** NAT gateway phải nằm ở public subnet(chọn public subnet vừa tạo)
  + **Connectivity type:** Public
  + **Elastic IP allocation ID:** Allocate Elastic IP
* Nhấn **Create subnet**

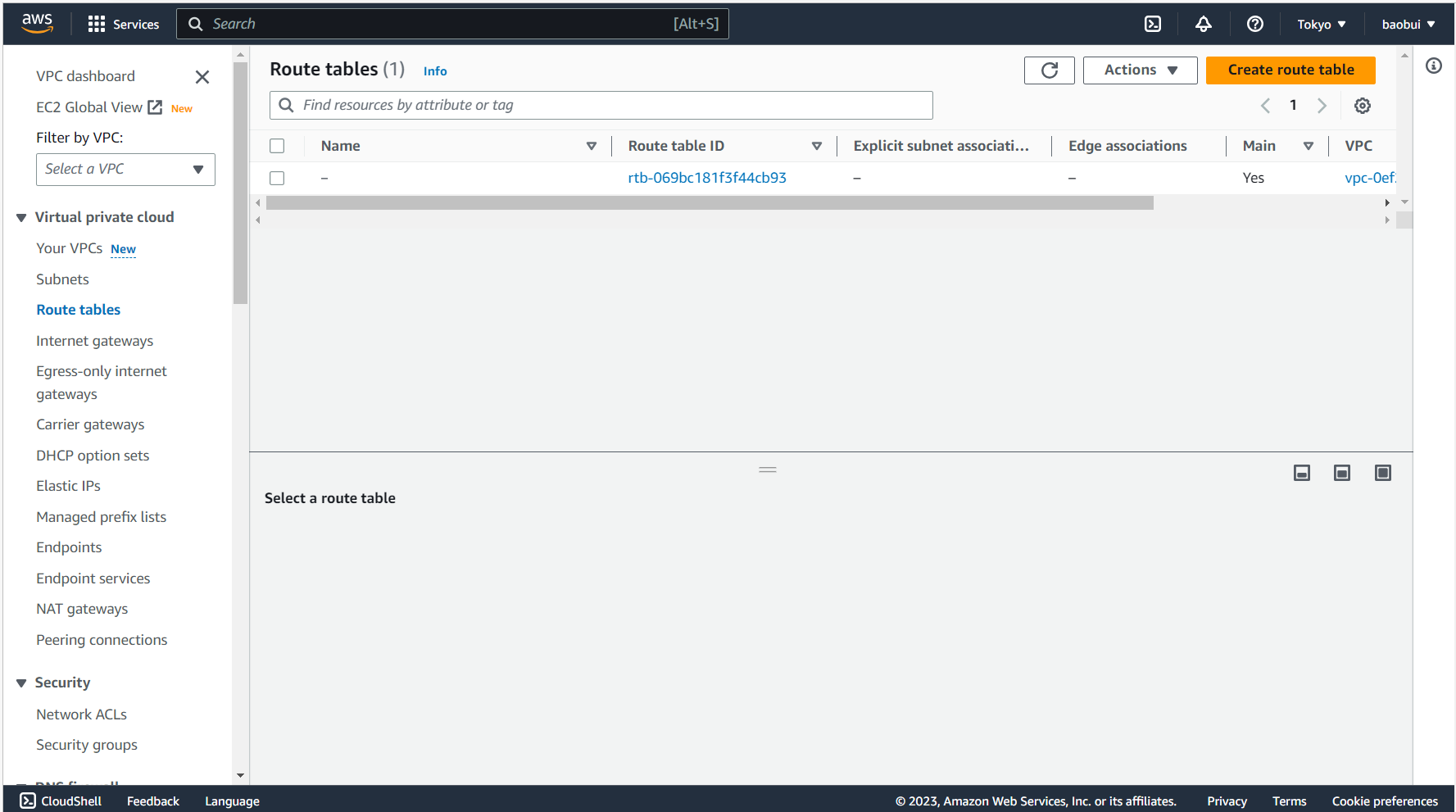


**Tạo thành công - thông tin/trạng thái của natgw**

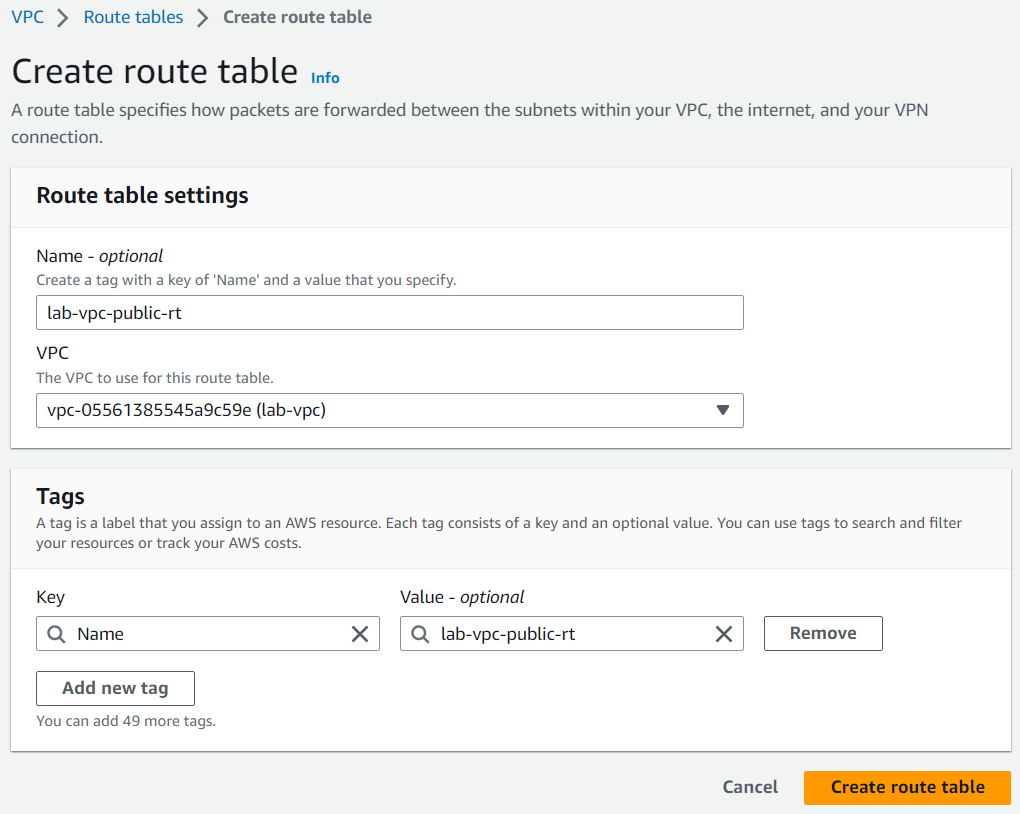


1. **Tạo route tables**

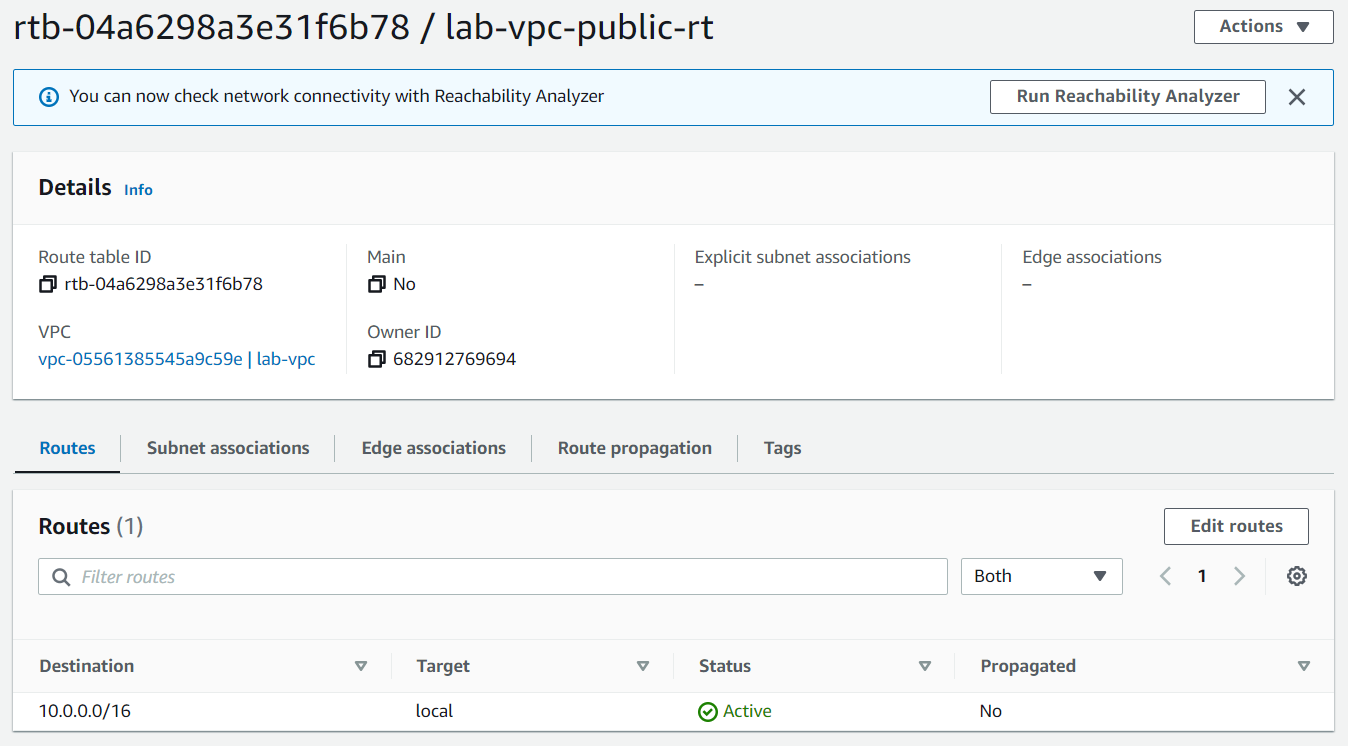
Truy cập [Route tables | VPC Management Console](https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-northeast-1#RouteTables:) và nhấn **Create route table**

****

* Thiết lập các cài đặt
  + **Name – optional**: đặt tên tương ứng(ở đây lab-vpc-public-rt).
  + **VPC**: Chọn VPC vừa tạo
* Nhấn **Attach route table**



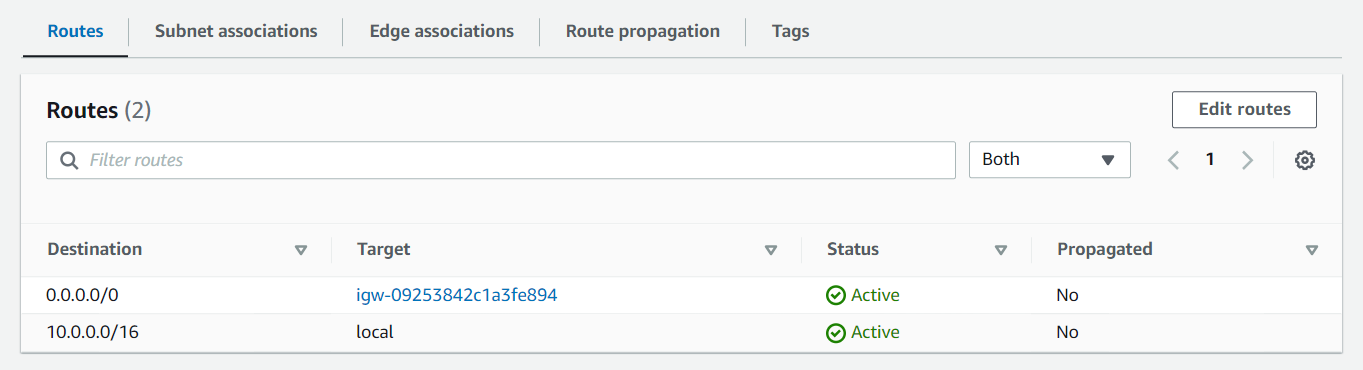
Tạo thành công và hiện tại chỉ có 1 route và target là **local** nên chưa thể truy cập được ra internet



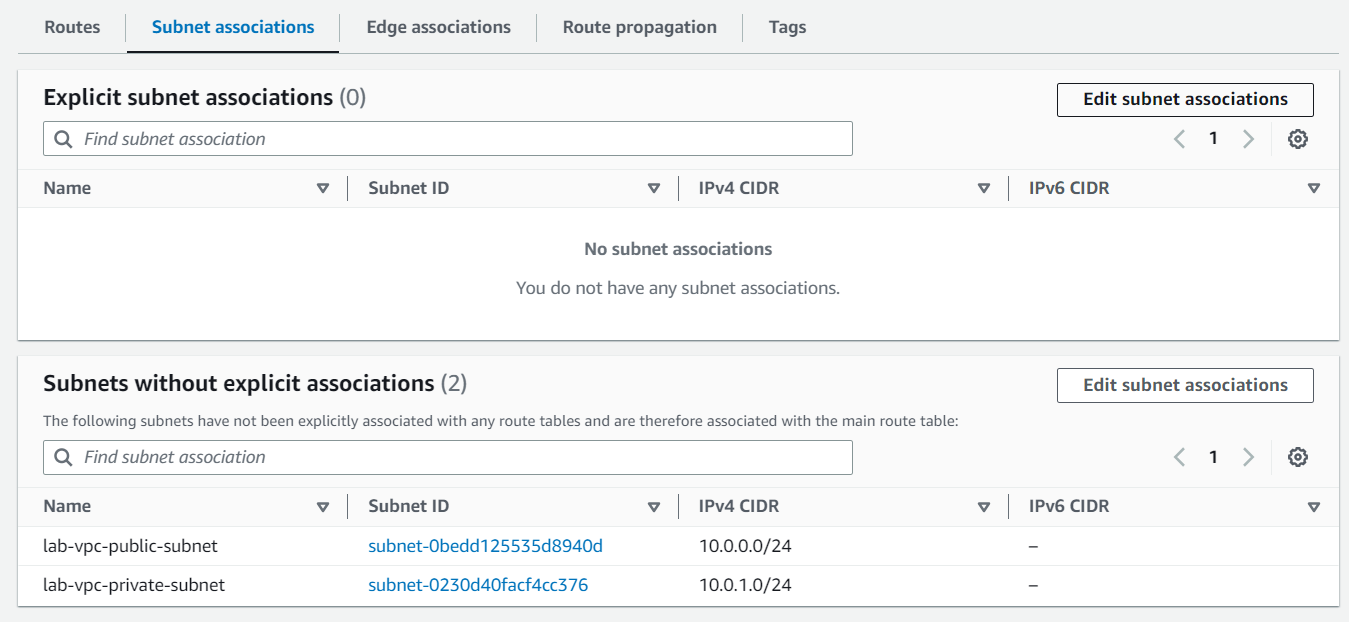
Tạo thêm route để có thể truy cập ra ngoài internet, chọn **Edit routes. Destination – 0.0.0.0/0** là tất cả các IPv4 và **Target – internet gateway** (Muốn đi ra ngoài phải đi qua cổng). **Nhấn Save Changes**



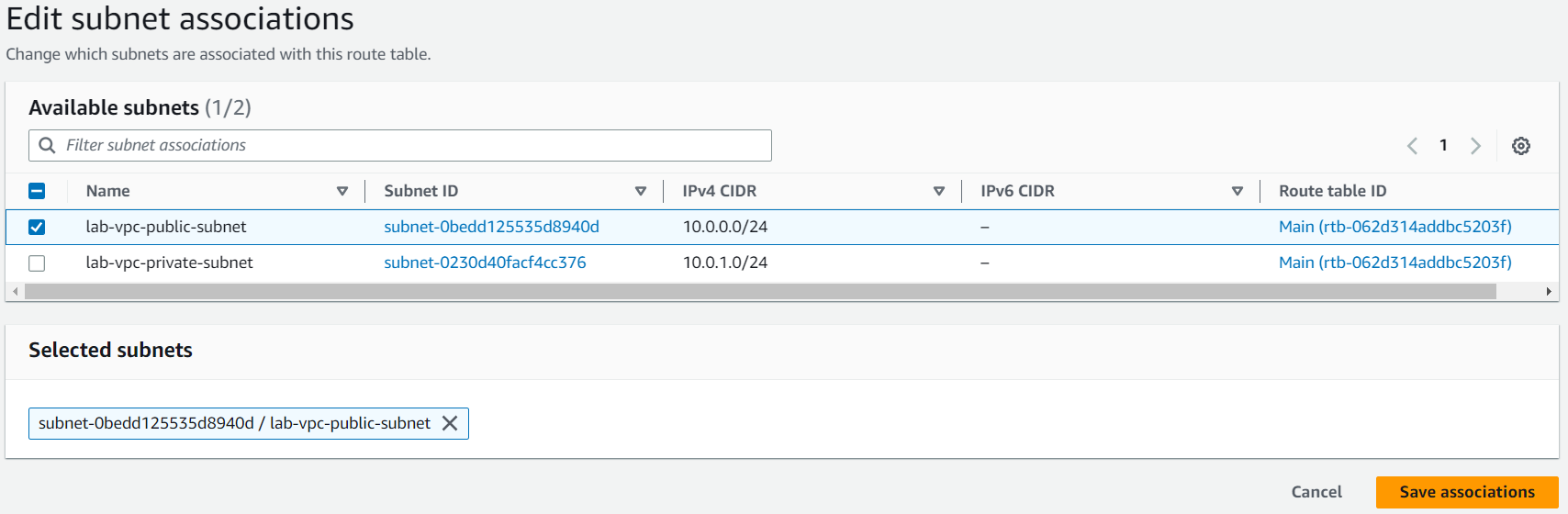
Cài đặt thành công, nhìn thấy có thêm 1 route



Tuy nhiên, cần chỉ định subnet nào sử dụng route để đi ra ngoài internet, nhấn chọn qua **Subnet associations**và chọn **Edit subnet associations**



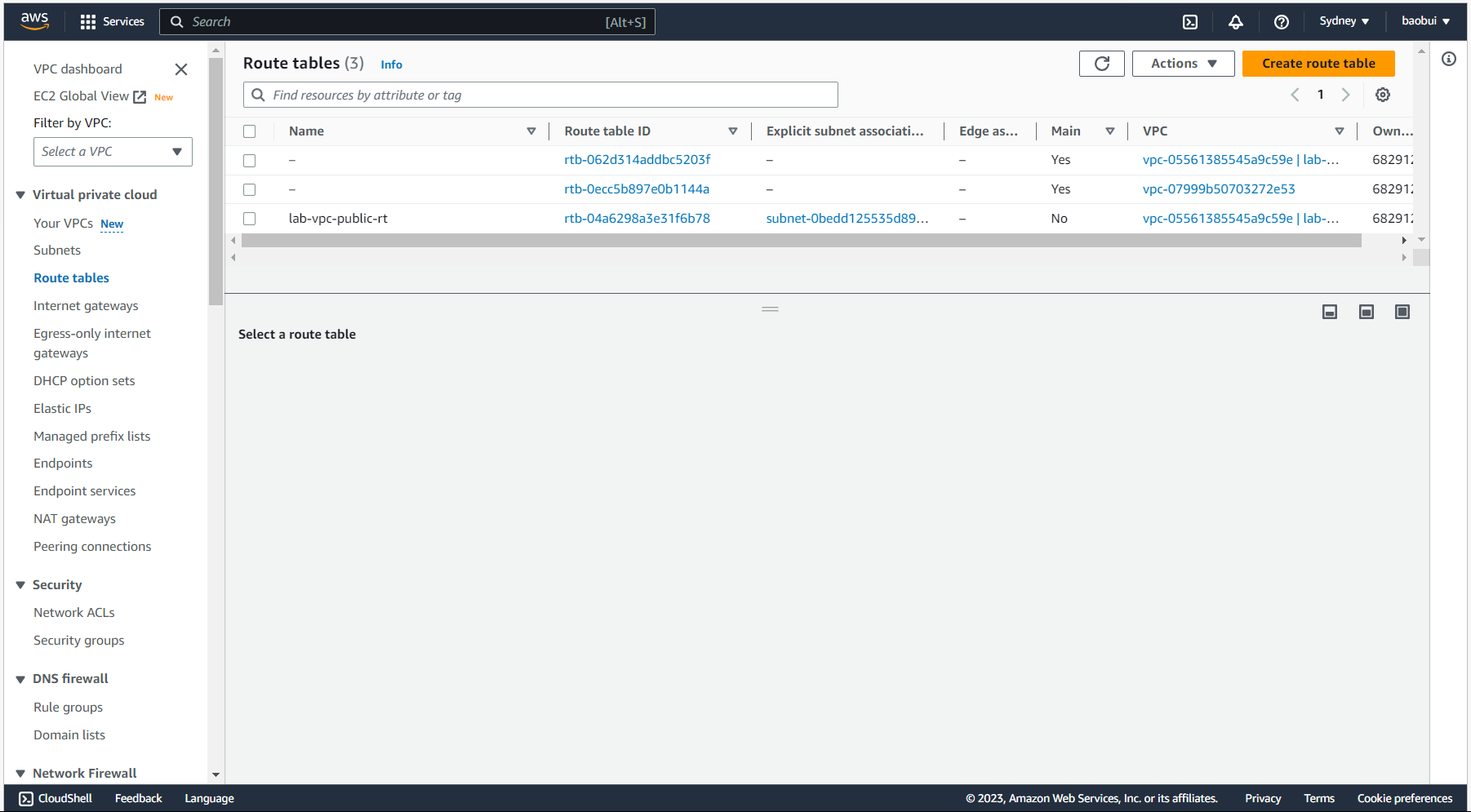
Ở chọn mạng con **lab-vpc-public-subnet** được phép truy cập ra vào internet. Nhấn **Save associations**



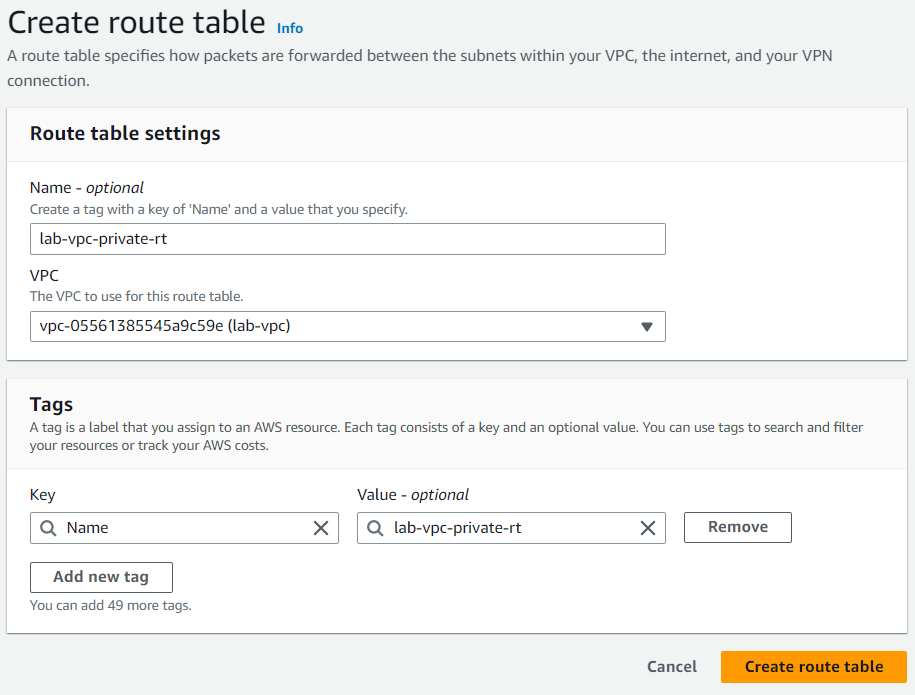
Kiểm tra route table đã được chỉ định cho mạng con



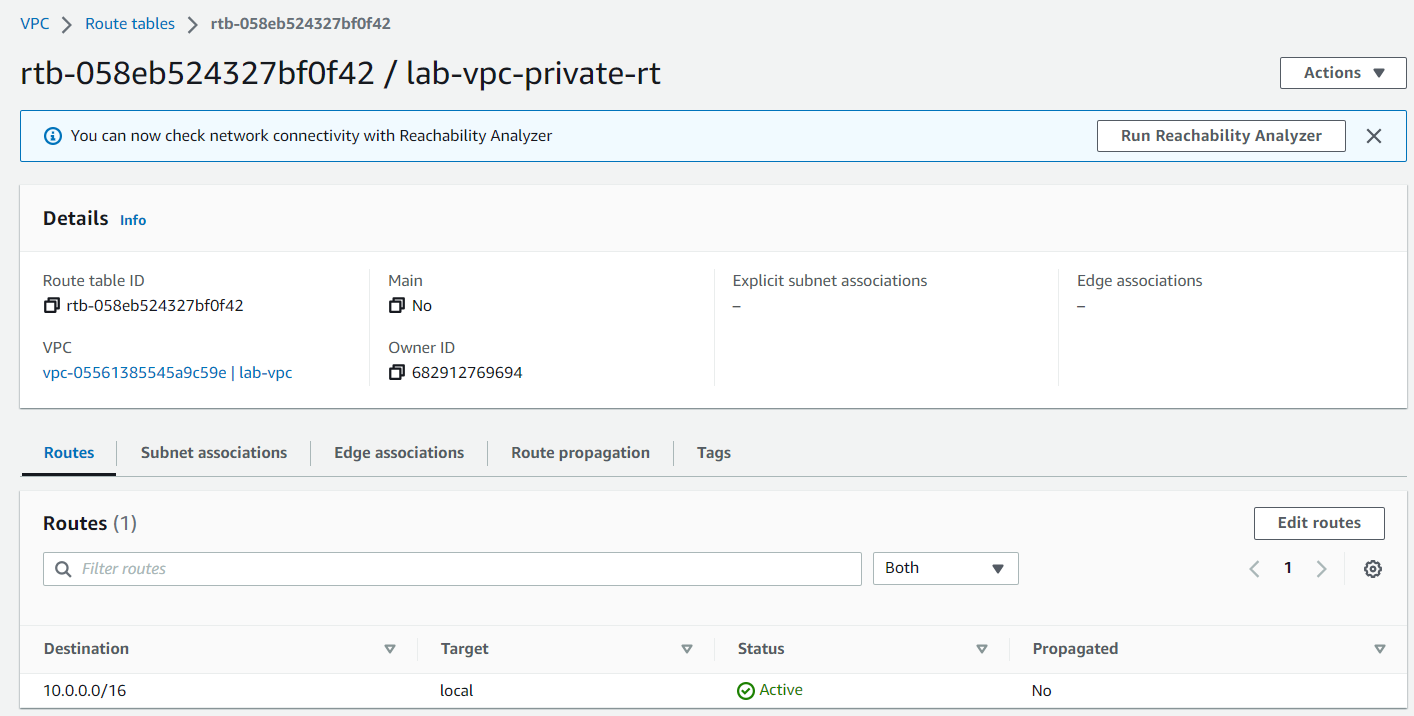
Tương tự, tạo thêm một route table cho mạng con private để route cổng NAT gateway



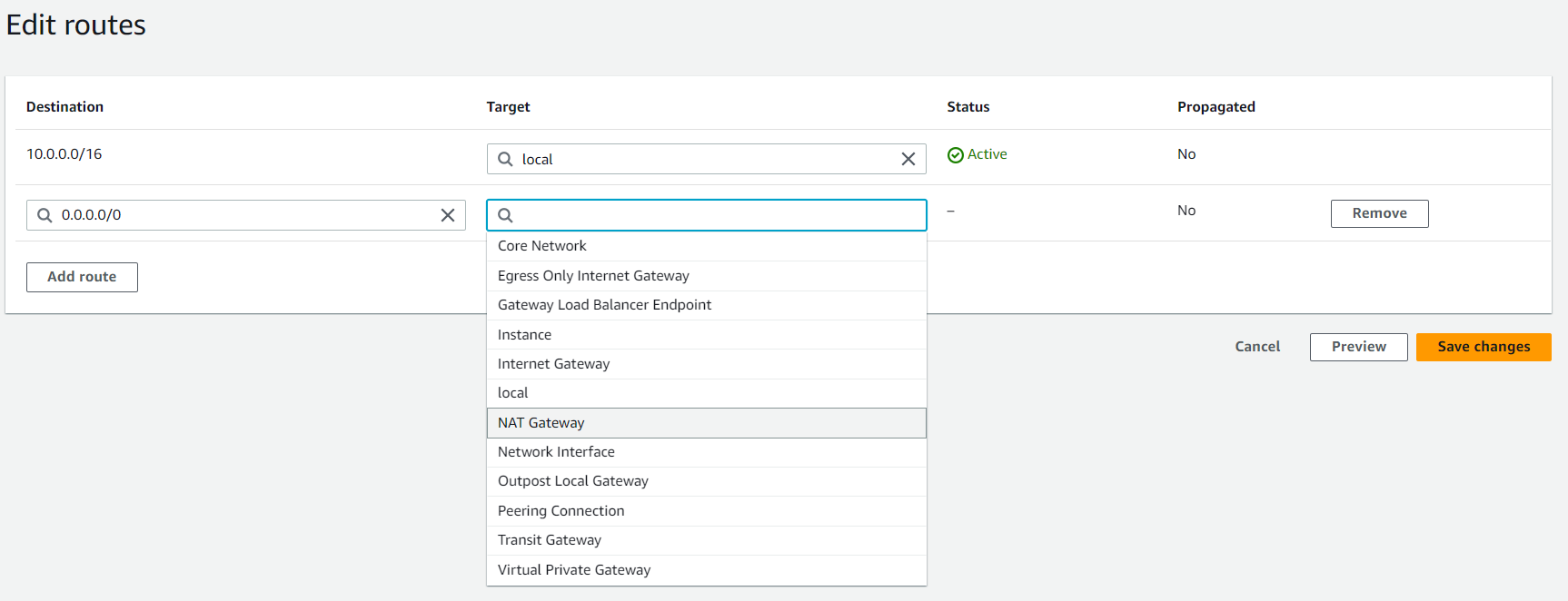
Đặt tên và chọn vpc vừa tạo



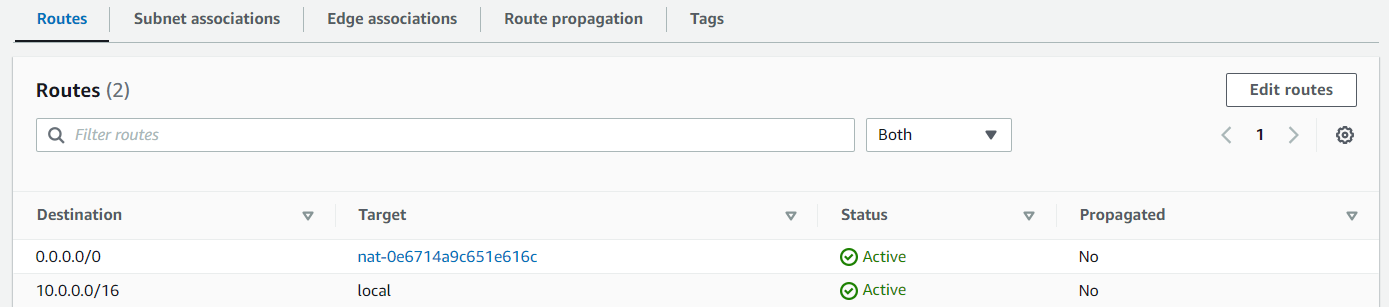
Tạo thành công, sau đó thêm một route cổng NAT gateway



Chọn cổng NAT gateway



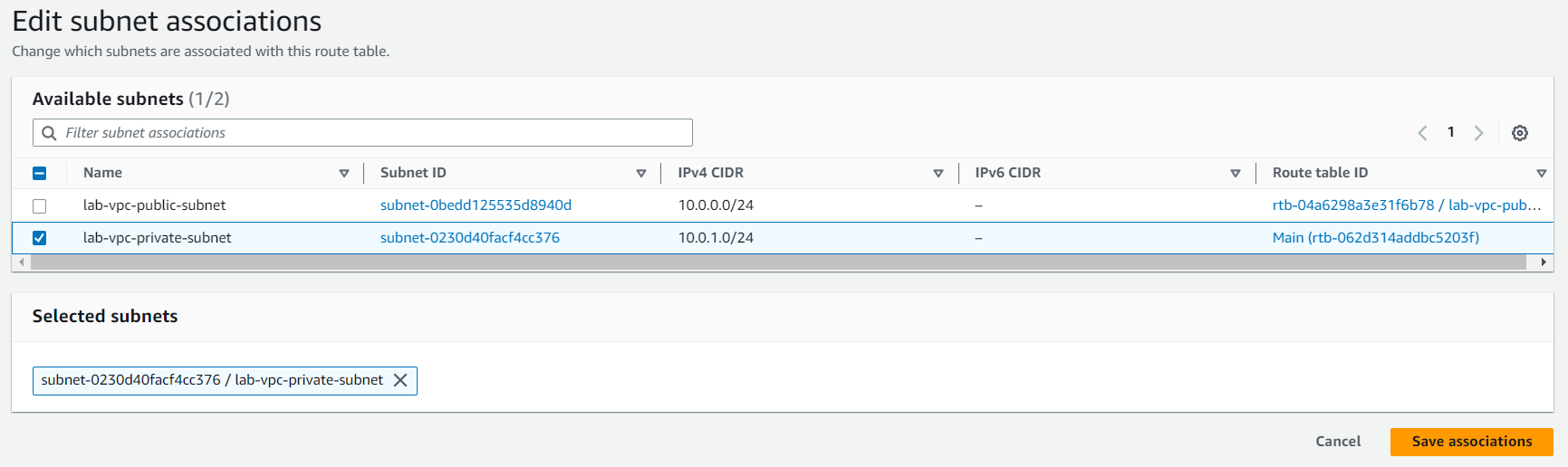
Thêm thành công 1 route



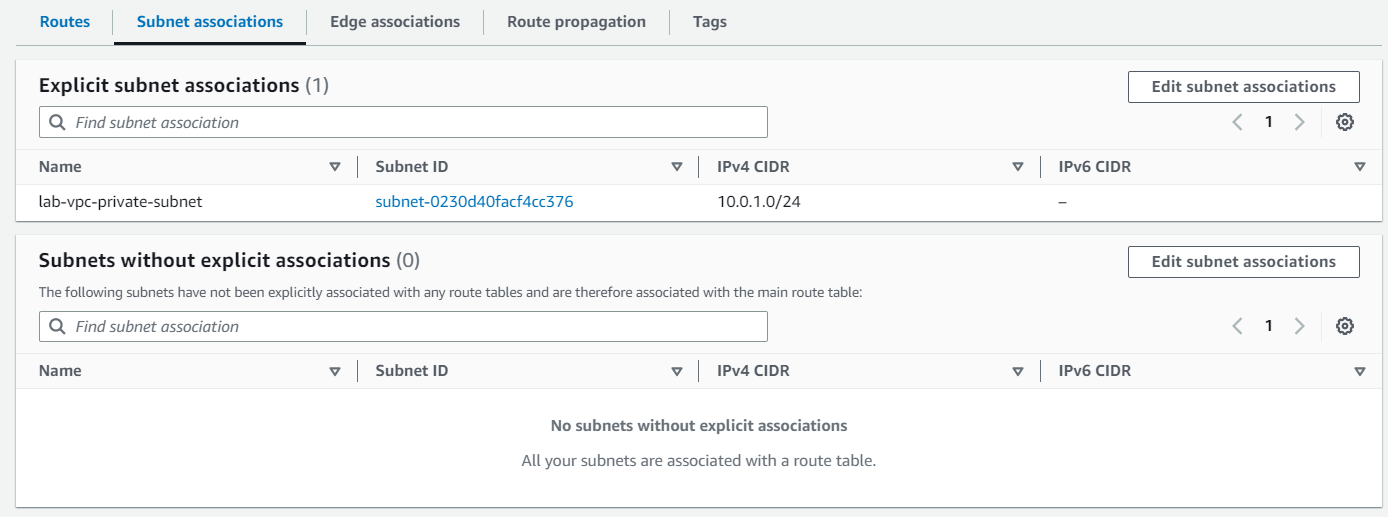
Chỉ định subnet private sử dụng route table này



Chọn mạng con private



Chỉ định thành công mạng con sử dụng route table này

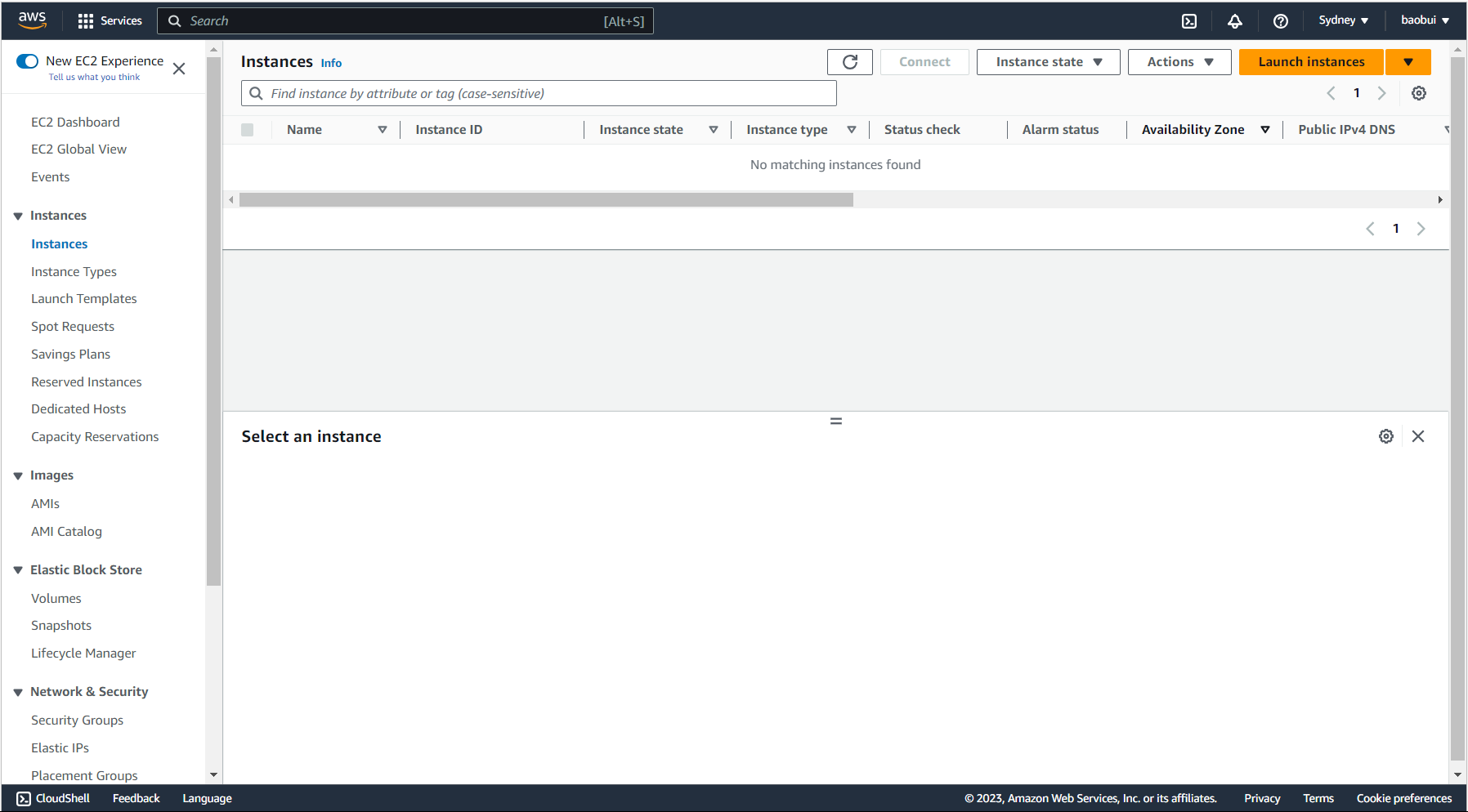


1. **Tạo EC2 máy chủ kiểm tra truy cập của VPC**

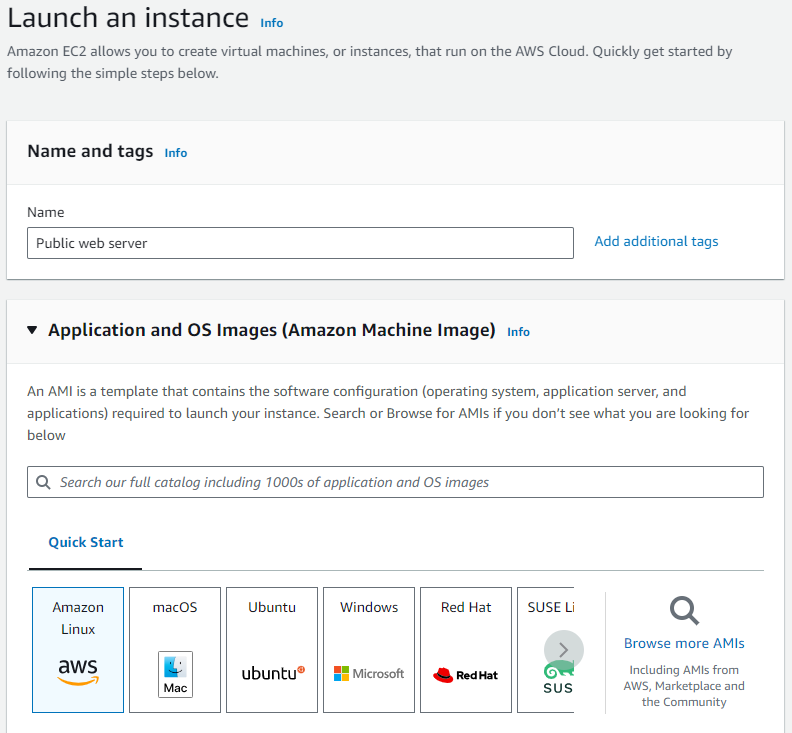
Ở đây đã tạo thành công mạng VPC, EC2 (Máy tính mạng nội bộ được phép truy cập internet) là 1 phần riêng lớn, nên không đi qua sâu chỉ tạo đơn giản đủ để kiểm được mạng VPC.

Tạo một máy chủ ở mạng con public

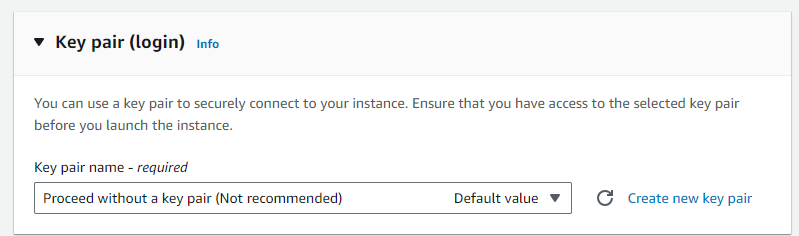
Truy cập [Dashboard | EC2 Management Console](https://ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Home:) và chọn **Launch instance**



Đặt tên và chọn hệ điều hành linux cho nhẹ



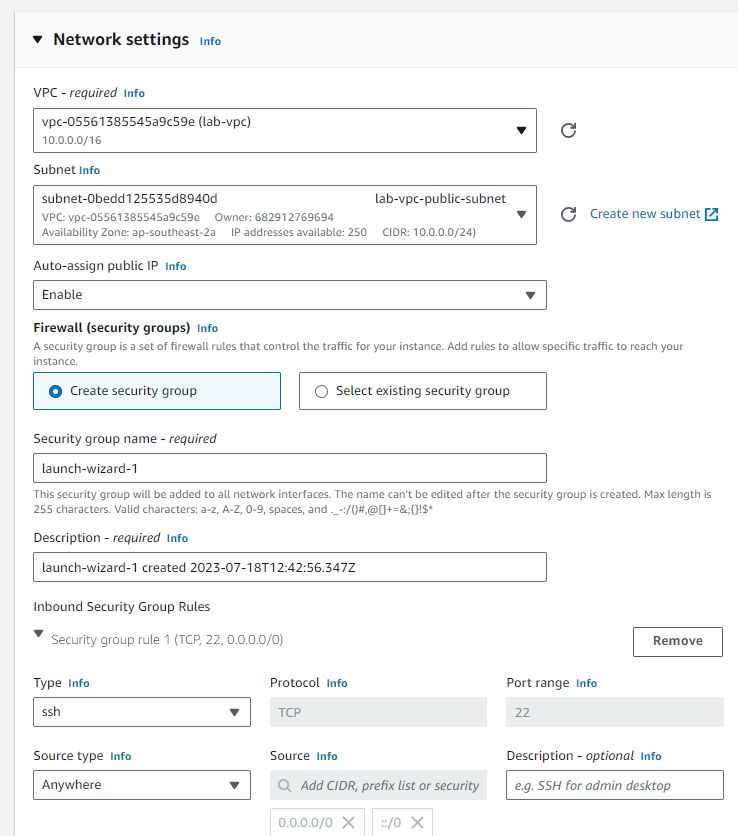
**Key pair(login):** chọn defalut value



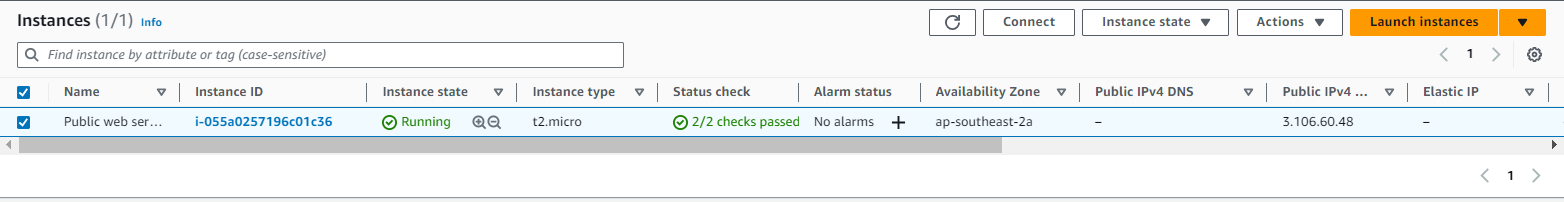
**Network settings:** nhấn Edit

* **VPC:** chọn vpc đã tạo
* **Subnet:** chọn mạng con public đã tạo
* **Auto-asign public Ip:** enable
* **Còn lại:** để mặc định

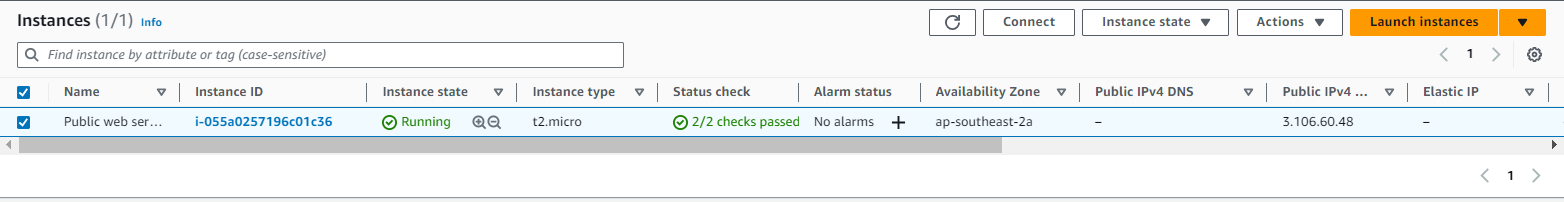
Nhấn **Launch instance**



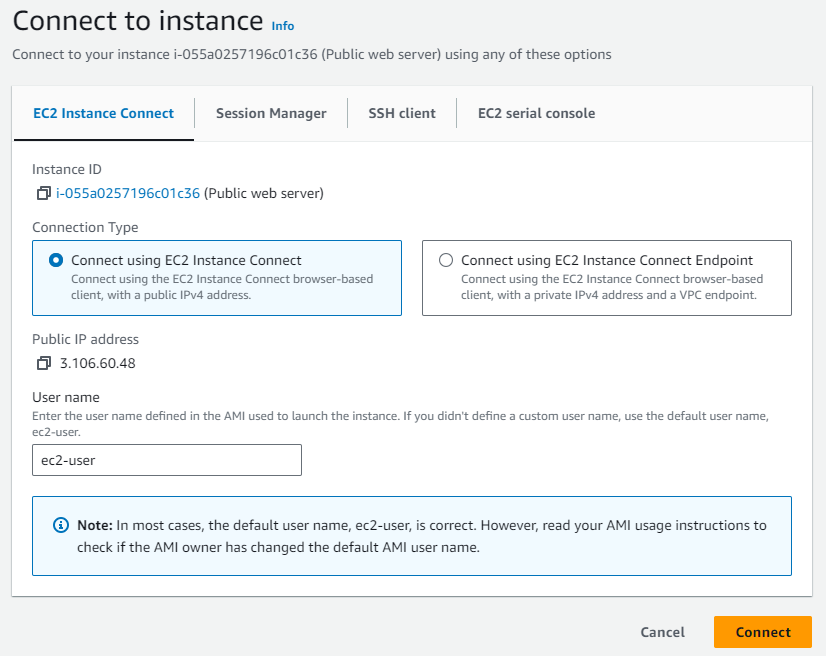
Tạo thành công



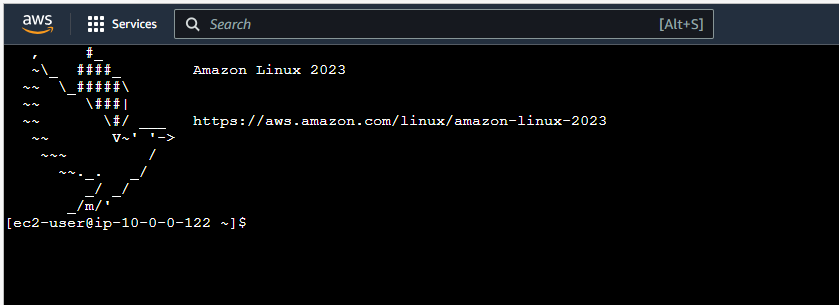
Tiến hành kết nối vào máy chủ: chọn Public web server và nhấn Connect



Tiếp tục nhấn Connect



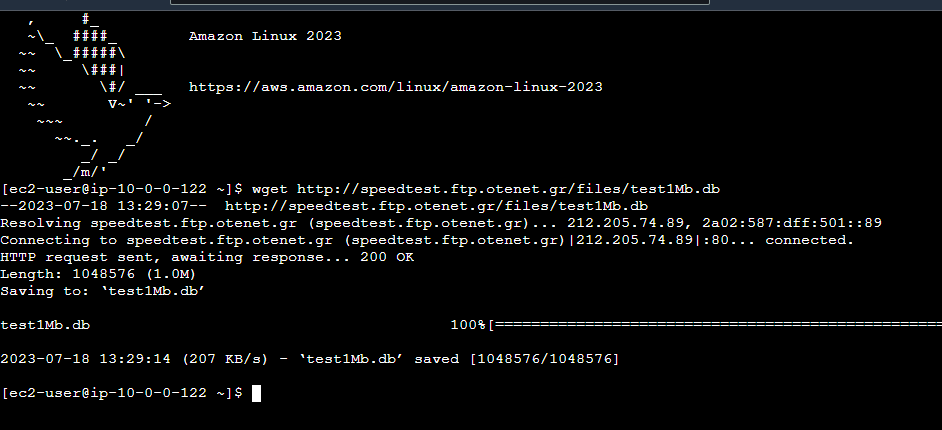
Truy cập thành công máy chủ web server, tiến hành kiểm tra truy cập



Kiểm tra truy cập ra ngoài internet: download thử 1 file từ web server sử dụng công cụ wget(Wget là một công cụ máy tính tạo ra từ GNU Project.Dùng nó để trích xuất dữ liệu và nội dung từ nhiều web servers khác nhau)

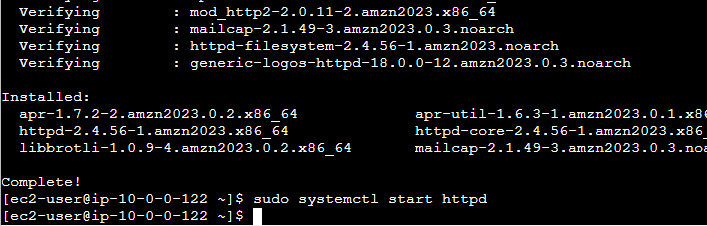
Link dùng để test: <http://speedtest.ftp.otenet.gr/files/test1Mb.db> (được lấy từ trang testfiledownload.com)

Tải thành công, vậy đã có thể đi ra ngoài internet

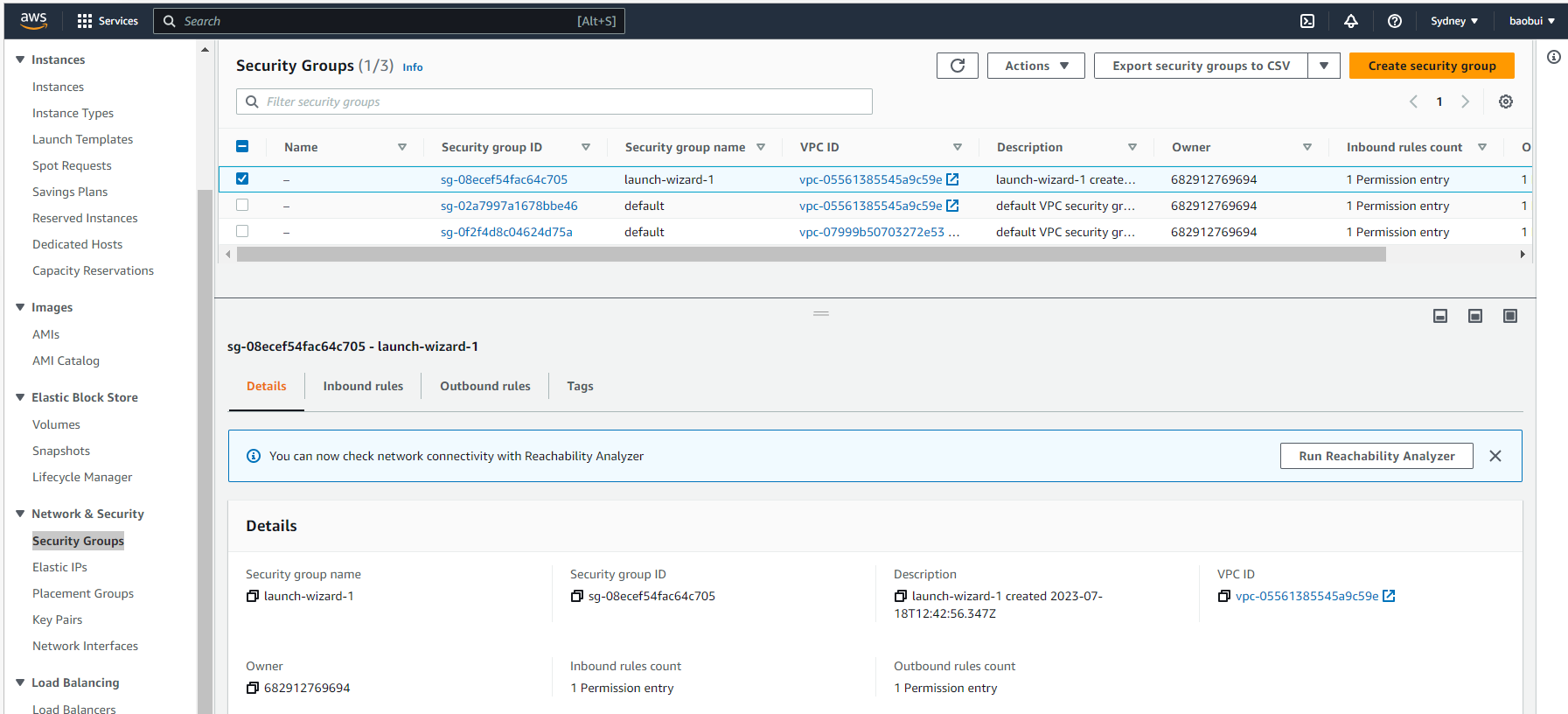


Kiểm tra truy cập đi từ internet đi vào: cài đặt web server trên máy chủ và dùng public ip của may máy chủ để hiện ra trang web, cài đặt dùng các câu lệnh:

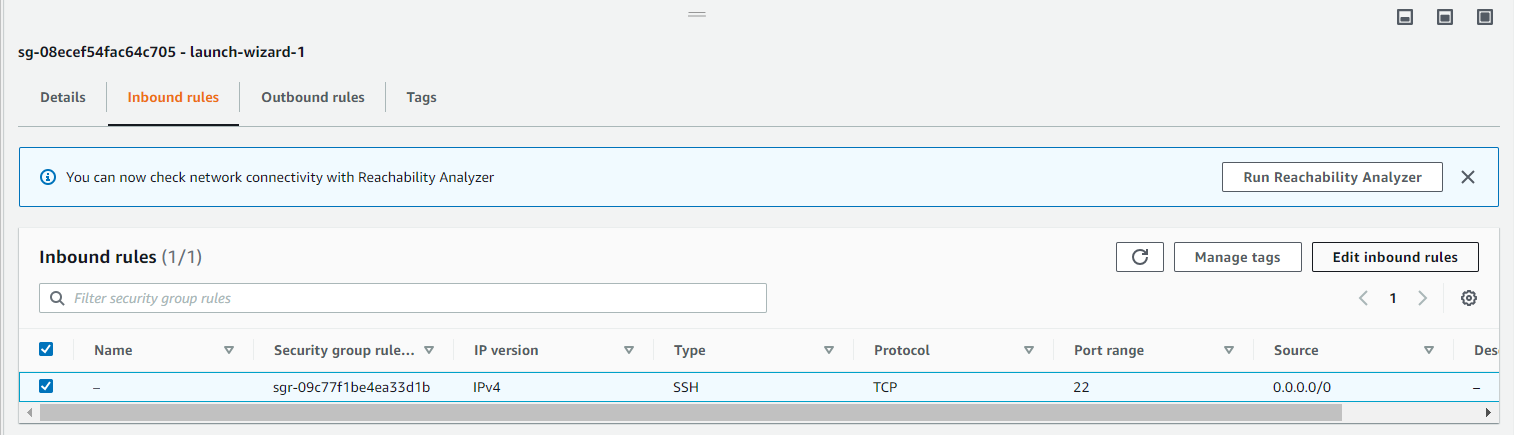
* sudo yum install httpd
* sudo systemctl start httpd



* Truy cập [Security Groups](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroups:), chọn launch-wizard-1



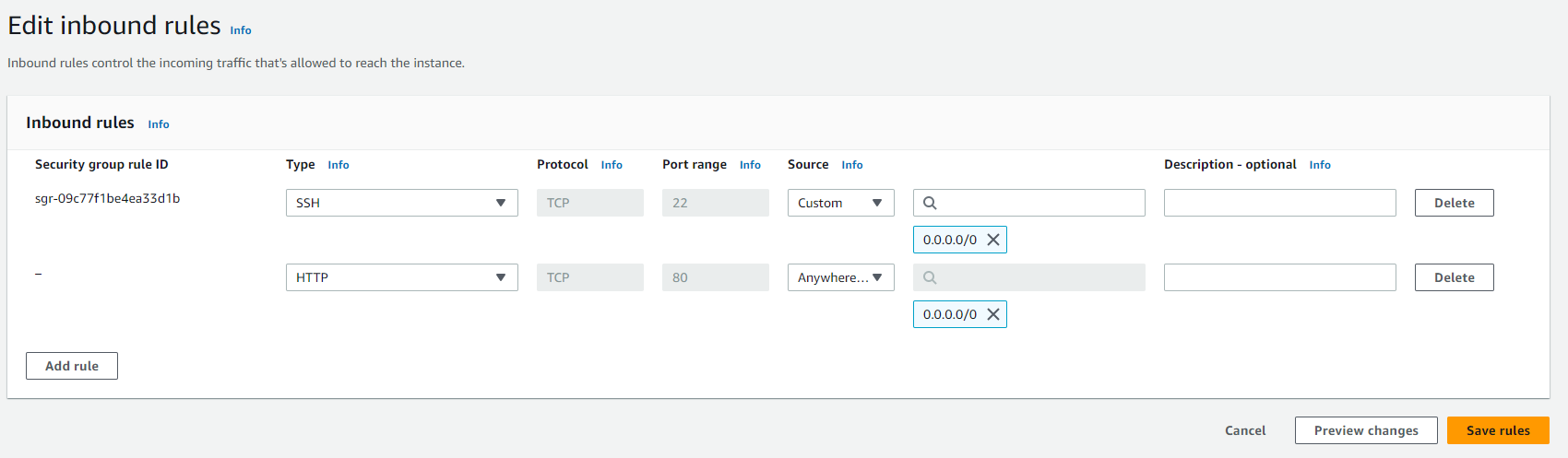
Chọn Inbound rules và nhấn Edit inbound rules



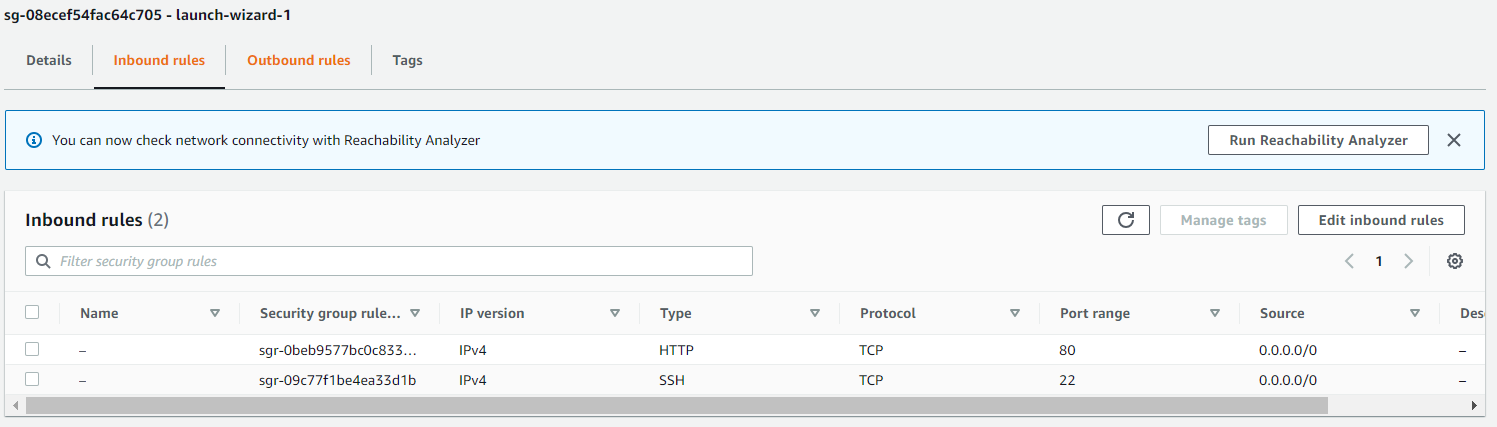
Nhấn Add rule, thiết lập:

* **Type:** HTTP
* **Source:** Anywhere-IPv4

Nhấn **Save rules**

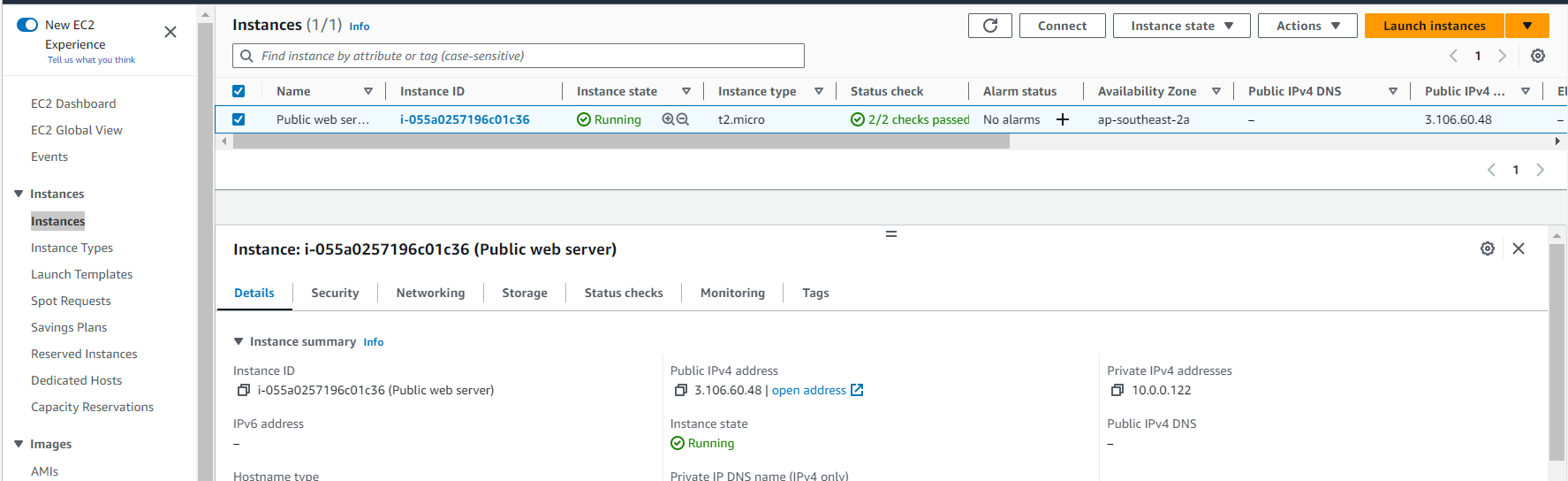


Thêm thành công một rule



Lấy địa chỉ ip public của web server để truy cập:

* Truy cập [Instances](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#Instances:), chọn public web server
* Địa chỉ ở Public IPv4 address(ở đây là 3.106.60.48)



Truy cập thành công, vậy có thể truy cập từ ngoài internet vào Server

