TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

Đề tài:

XÂY DỰNG CHUỖI CHỨC NĂNG MẠNG ẢO HÓA (SFC) TRÊN NỀN TẢNG OPENSTACK

Sinh viên thực hiện: NGUYỄN THỊ THANH TÂM
LỚP ĐTTT 06 – K58
Giảng viên hướng dẫn: TS. NGUYỄN XUÂN DŨNG

Hà Nội, 6-2018

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

Đề tài:

XÂY DỰNG CHUỖI CHỨC NĂNG MẠNG ẢO HÓA (SFC) TRÊN NỀN TẢNG OPENSTACK

Sinh viên thực hiện: NGUYỄN THỊ THANH TÂM
LỚP ĐTTT 06 – K58
Giảng viên hướng dẫn: TS. NGUYỄN XUÂN DŨNG
Cán bộ phản biện:

Hà Nội, 6-2018

Đánh giá quyển đồ án tốt nghiệp

(Dùng cho giảng viên hướng dẫn)

Giảng viên đánh giá: TS. Nguyễn Xuân Dũng

Họ và tên Sinh viên: Nguyễn Thị Thanh Tâm MSSV: 20133430

Tên đồ án: Xây Dựng Chuỗi Chức Năng Mạng Ảo Hóa (SFC) Trên Nền Tảng Openstack

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây: Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5
6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, em chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5
9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				
Điểm tổng		**/50**				
Điểm tổng quy đổi về thang 10						

Nhận xét thêm của Thầy/Cô (*giảng viên hướng dẫn nhận xét về thái độ và tinh thần làm việc của sinh viên****)***

.....

.....

.....

.....

.....

.....

Ngày: / /201

Người nhận xét

(Ký và ghi rõ họ tên)

Đánh giá quyển đồ án tốt nghiệp

(Dùng cho cán bộ phản biện)

Giảng viên đánh giá: .....

Họ và tên Sinh viên: Nguyễn Thị Thanh Tâm MSSV: 20133430

Tên đồ án: Xây Dựng Chuỗi Chức Năng Mạng Ảo Hóa (SFC) Trên Nền Tảng Openstack.

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5
6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, em chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5
9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				
Điểm tổng		**/50**				
Điểm tổng quy đổi về thang 10						

3. Nhận xét thêm của Thầy/Cô

.....
.....
.....
.....
.....
.....

Ngày: / /201

Người nhận xét

(Ký và ghi rõ họ tên)

LỜI NÓI ĐẦU

Với sự phát triển nhanh chóng của Internet và các công nghệ như thời điểm hiện nay, việc phát triển thêm các dịch vụ giá trị gia tăng (VAS - Value-Added Services) cho các khách hàng của mình dần trở thành ưu tiên hàng đầu của các nhà cung cấp dịch vụ. Để cung cấp một dịch vụ đầu cuối hoàn chỉnh cho khách hàng, các nhà cung cấp dịch vụ mạng viễn thông và công nghệ thông tin phải thiết lập và cấu hình hệ thống các dịch vụ mạng, chức năng mạng phù hợp để đảm bảo dịch vụ tới người dùng hoạt động ổn định, tin cậy. Với sự phát triển nhanh chóng của công nghệ Ảo hóa chức năng mạng (NFV) và Công nghệ mạng định nghĩa bằng phần mềm (SDN), việc triển khai các chuỗi dịch vụ mạng đã trở thành giải pháp tuyệt vời cho các nhà cung cấp mạng thay đổi linh hoạt cách thức phục vụ người dùng với nhiều mô hình dịch vụ khác nhau.

Vì vậy, sau quá trình học tập tại trường, đồng thời nhận được sự chỉ dẫn tận tính của thầy Nguyễn Xuân Dũng cũng như các thầy cô trong Viện Điện tử Viễn thông, em xin chọn đề tài: “Xây dựng chuỗi chức năng mạng ảo hóa trên môi trường Openstack” để làm đồ án tốt nghiệp.

Em xin chân thành cảm ơn TS. Nguyễn Xuân Dũng đã tận tình giúp đỡ, tạo điều kiện để em thực hiện Đề tài thực tập tốt nghiệp. Ngoài ra em cũng cũng xin chân thành cảm ơn thầy Nguyễn Hữu Thanh cùng các thành viên Future Internet Lab đặc biệt là các bạn trong nhóm Network Function Virtualization đã giúp đỡ, chia sẻ trong suốt thời gian qua.

TÓM TẮT ĐỒ ÁN

Chuỗi chức năng dịch vụ (Service Function Chaining - SFC) là công nghệ quy định các chính sách chuyển tiếp lưu lượng tách biệt trong vùng chuỗi dịch vụ. Chuỗi các chức năng dịch vụ mạng SFC định nghĩa và tạo ra một chuỗi các dịch vụ mạng theo thứ tự mong muốn và điều khiển lưu lượng truy cập thông qua chúng. Hiện nay, kiến trúc mạng của các nhà khai thác mạng được phân bổ nhiều thiết bị phần cứng độc quyền. Ứng với mỗi loại dịch vụ, mỗi chức năng mạng lại có các thiết bị phần cứng chuyên trách đảm nhận. Các thiết bị này còn đang có một số hạn chế như: chi phí thiết bị cao, khó quản lý tập trung, độ tương thích thấp với hệ thống của nhiều hãng khác dẫn tới doanh nghiệp phải phụ thuộc vào một số hãng phần cứng nhất định.

Trong đồ án này, em trình bày về công nghệ ảo hóa chức năng mạng (NFV) và các lợi ích của chuỗi dịch vụ mạng (SFC), các trường hợp sử dụng hai công nghệ đó đem lại lợi ích như thế nào cho các nhà cung cấp dịch vụ mạng và khách hàng. Đồng thời, em cũng xây dựng hệ thống chuỗi chức năng mạng sử dụng các chức năng mạng ảo hóa ở quy mô nhỏ để kiểm thử các tính năng và đánh giá hiệu năng hoạt động của chuỗi chức năng.

ABSTRACT

Service Function Chaining (SFC) is a technology that governs traffic separation policies in the service chain area. The service function network defines and creates a sequence of network services in the desired order and controls the traffic through them. At present, the network infrustracture of the network operators are distributed many proprietary hardware devices. Corresponding to each type of service, each network function has specialized hardware undertake. These devices have a number of limitations: high cost of equipment, difficulty in centralized management, low compatibility with many other systems leading to the enterprise depends on some hardware vendors regulations.

In this project, I present the definition of NFV and the benefits of the network service chain (SFC), the use cases of two technologies and the benefits that they bring to network service providers and customers. At the same time, I also built a testbed about network functional sequence system using small-scale network virtualization functions to test the features and assess the performance of SFC.

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH SÁCH CÁC BẢNG BIỂU

DANH SÁCH CÁC TỪ VIẾT TẮT

1. CHƯƠNG 1: MỞ ĐẦU

1.1. Đặt vấn đề

1.2. Đề xuất hướng giải quyết

2. CHƯƠNG 2: CƠ SỞ LÝ THUYẾT CHUNG

2.1. Tổng quan về công nghệ điện toán đám mây

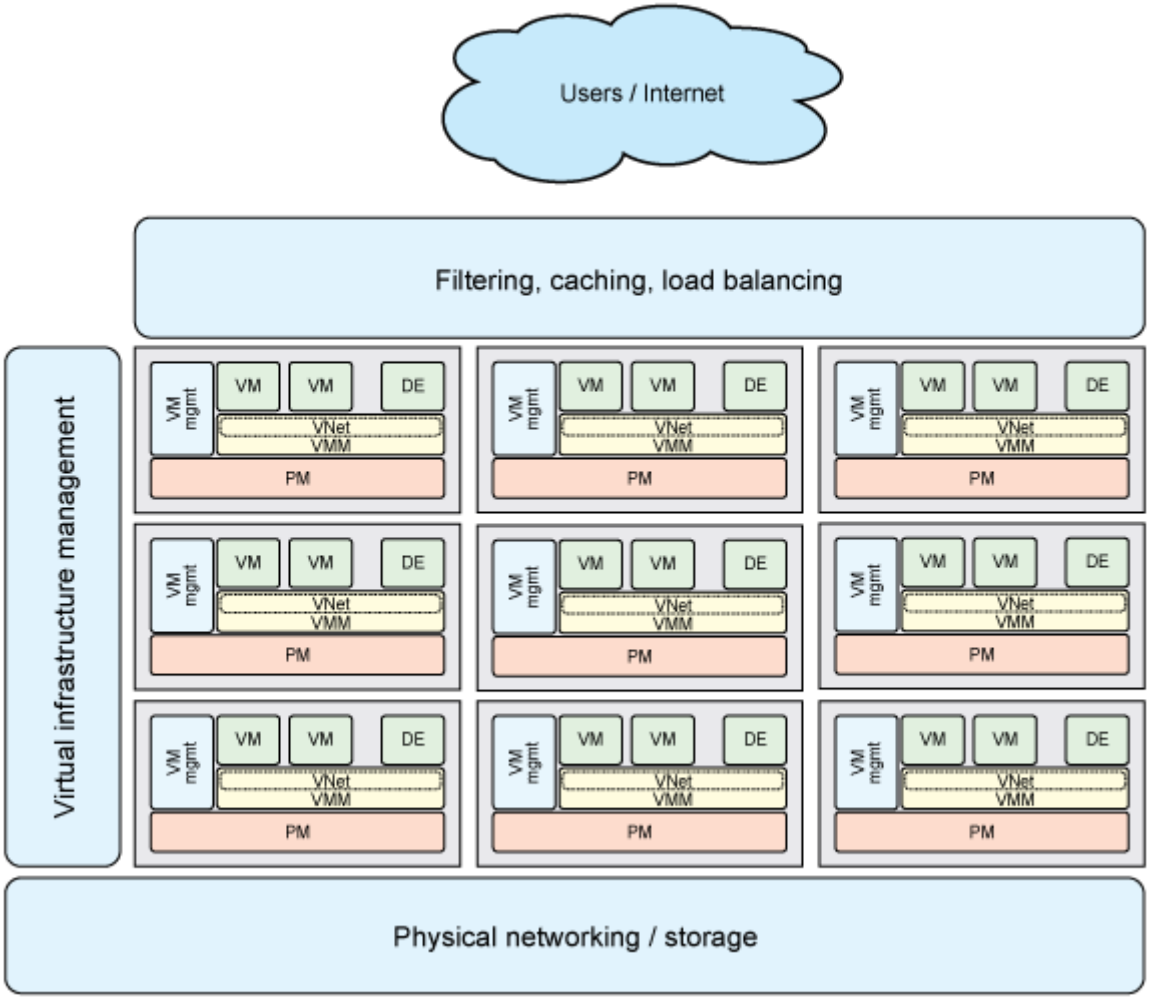
2.1.1. Giới thiệu về công nghệ điện toán đám mây

Điện toán đám mây (Cloud Computing), còn gọi là điện toán máy chủ ảo: là mô hình tính toán sử dụng các công nghệ máy tính và phát triển dựa vào mạng Internet.

Thuật ngữ ***"Cloud Computing"*** ra đời giữa năm 2007, dùng để khái quát lại các hướng phát triển của cơ sở hạ tầng CNTT vốn đã và đang diễn ra từ nhiều năm qua. Quan niệm này có thể được diễn giải một cách đơn giản như sau: các nguồn tài nguyên tính toán khổng lồ như các phần cứng (máy chủ), phần mềm, và các dịch vụ (chương trình ứng dụng), … sẽ nằm tại các máy chủ ảo (đám mây - cloud) trên Internet thay vì trong máy tính gia đình và văn phòng (trên mặt đất) để mọi người kết nối và sử dụng mỗi khi họ cần dù ở bất cứ đâu miễn có kết nối Internet.

Nói cách khác, đây là một mô hình cho phép truy cập qua mạng để chia sẻ chung nguồn tài nguyên (mạng, dịch vụ, ứng dụng, máy chủ, không gian lưu trữ, …) một cách nhanh chóng, thuận tiện và đồng thời cho phép kết thúc sử dụng dịch vụ, giải phóng tài nguyên dễ dàng, giảm thiểu sự ảnh hưởng quản lý và giao tiếp với nhà cung cấp. Mọi khả năng liên quan đến công nghệ thông tin đều được cung cấp dưới dạng các "dịch vụ", cho phép người sử dụng truy cập các dịch vụ công nghệ thông tin từ một nhà cung cấp nào đó "trong đám mây" mà không cần phải biết về công nghệ đó, cũng như không cần quan tâm đến các cơ sở hạ tầng phục vụ công nghệ đó.

Điện toán đám mây được hình thành bằng cách kết hợp công nghệ ảo hóa trên các nút máy chủ vật lý lại với nhau trên mạng vật lý, kết hợp lưu trữ có chia sẻ và phối hợp quản lý trên toàn bộ cơ sở hạ tầng, rồi cung cấp cân bằng tải. Mô hình cơ sở hạ tầng của điện toán đám mây được mô tả trong hình sau:



Hình 2.1: Mô hình cơ sở hạng tầng của điện toán đám mây

2.1.2. Các đặc trưng của công nghệ điện toán đám mây

Mô hình điện toán đám mây – Cloud Computing đặc trưng bởi 5 đặc tính, 3 mô hình dịch vụ và 4 mô hình triển khai.

5 đặc tính:

- ***On-demand self service :*** Khả năng tự phục vụ : người dùng có khả năng tự tính toán được nhu cầu sử dụng máy chủ lưu trữ, khi cần thiết có thể thực hiện tự động mà không cần phải có sự giao tiếp với nhà cung cấp dịch vụ.
- ***Broad network access:*** khả năng truy cập nhiều kiểu hạ tầng mạng khác nhau, hỗ trợ nhiều nền tảng thiết bị, nhiều hạ tầng vật lý (như điện thoại di động, laptop, tablet, máy trạm..)

- ***Resource pooling:*** Dùng chung tài nguyền mạng. Tài nguyên tính toán được của nhà cung cấp được dùng chung cho nhiều khách hang sử dụng dịch vụ đa thuê bao, với những nguồn tài nguyên vật lý và ảo khác nhau được phân công và bố trí theo nhu cầu của người sử dụng. Khách hàng không thể xác định và biết được vị trí chính xác của nguồn tài nguyên nhưng mà có thể dễ dàng xác dịnhđược vị trí cung cấp nguồn tài nguyên một cách tương đối (quốc gia, liên bang, trung tâm dữ liệu).

  Gộp chung nguồn tài nguyên của nhiều máy chủ với nhau thành một khối thống nhất, rồi sau đó sẽ san sẻ tài nguyên cho người dùng. (mục đích dễ quản lý, cấp phát tài nguyên dễ dàng, nhanh chóng).

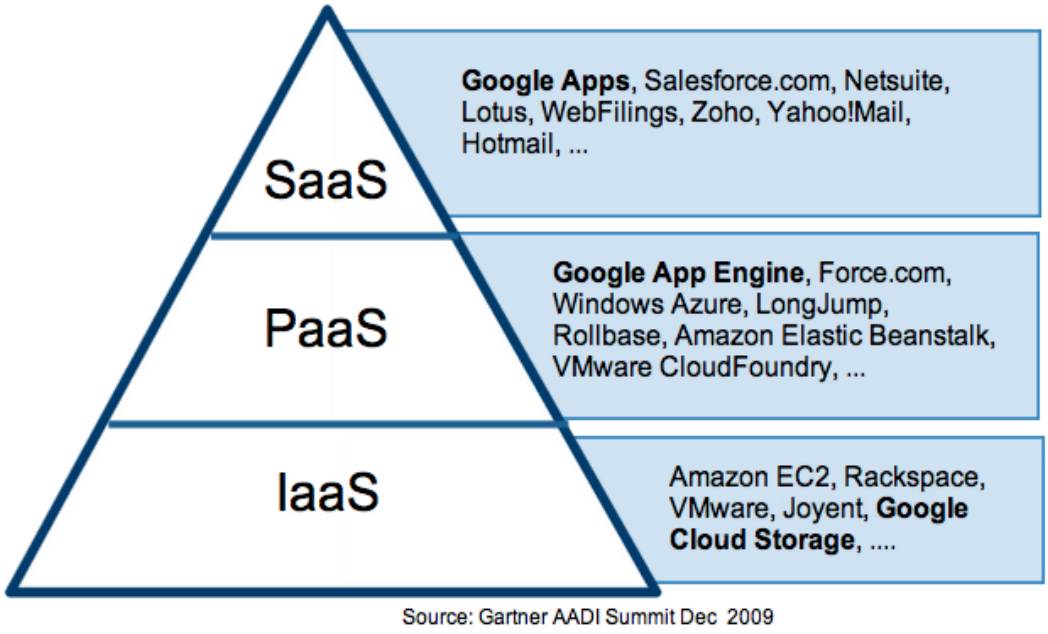
- ***Rapid Elasticity*** (có tính đàn hồi cao) : Có khả năng cung cấp và giải phóng tài nguyên một cách nhanh chóng, trong một số trường hợp có thể tự động thu hẹp hoặc mở rộng phạm vi tùy nhu cầu người dùng. Khách hàng có khả năng có thể được cung cấp không giới hạn và chiếm tài nguyên bất kì lúc nào.
- ***Measured service*** (Tính toán dịch vụ) : Hệ thống cloud tự động điều khiển và tối ưu hóa nguồn tài nguyên sử dụng bằng tận dụng khả năng đo lường ở một vài cấp độ dịch vụ. tính toán mức độ sử dụng dịch vụ, kiểm soát thời gian phục vụ, giám sát, điều khiển, báo cáo, etc. Từ đó có thể tính toán được chi phí của người sử dụng.

4 mô hình triển khai:

- ***Private cloud :*** Nền tảng cloud được cung cấp độc quyền cho 1 tổ chức bao gồm nhiều đối tượng (như công ty kinh doanh..). Nó có thể được làm chủ, điều khiển và vận hành bởi một tổ chức - môt thành viên thứ 3, hoặc là có sự kết hợp giữa 2 bên, có thể tồn tại hoặc không …
- ***Community cloud:*** Nền tảng cloud được cung cấp độc quyền cho một tổ chức người sử dùng đến từ các tổ chức có chung một mối quan tâm về mục đích, nhiệm vụ, chính sách. Nó có thể được quản lý, vận hành bởi một hoặc nhiều tổ chức trong cộng đồng kết hợp quản lý với nhau.

- ***Public Cloud:*** Hạ tầng Cloud đc cung cấp cho tất cả mọi người dùng thông thường. Được làm quản lý và vận hành bởi chính người dùng, có tính chất thương mại.. Có sự ràng buộc giữa người dùng và nhà cung cấp.
- ***Hybrid Cloud:*** Đây là hạ tầng cloud được phối hợp giữa 2 hoặc nhiều hạ tầng cloud riêng biêt. Những hạ tầng này vẫn giữ đặc điểm riêng biệt nhưng có thể phối hợp cùng nhau bởi việc được chuẩn hóa hoặc công nghệ phù hợp mà dữ liệu và ứng dụng có thể lưu động được.

3 mô hình dịch vụ:



Hình 2.2: 3 mô hình dịch vụ của điện toán đám mây

Như mô tả trên Hình 2.2, các mô hình dịch vụ của điện toán đám mây bao gồm:

- ***SaaS (Software as a Service):*** Khách hàng sử dụng những ứng dụng chạy trên nền tảng cloud của nhà cung cấp**.** Các ứng dụng có thể truy cập được từ các thiết bị thông qua giao diện với người dùng, Khách hang không có quyền quản lý và điều khiển kiến trúc hạ tầng của cloud như mạng, server, lưu trữ, hệ thống vẫn hành và thậm chí cả một vài ứng dụng cá nhân … do đó hạn chế người dùng về việc cáu hình đặc biệt cho các ứng dụng. (người dùng không cần quan

tâm xem cloud triển khai như thé nào, chỉ cần thuê và sử dụng dịch vụ thông qua các phần mềm client (web browser..)

- ***PaaS (Platform as a Service) :*** Nền tảng như một dịch vụ. cung cấp các dịch vụ về nền tảng, môi trường lập trình, database, etc. để khách hàng phát triển các ứng dụng của mình (thông thường nền tảng này cung cấp cho các developer). Ví dụ: AWS, GAE, Azue, Bluemix, OpenShift, etc.. Nhưng khách hàng không được quản lý các kiến trúc hạ tầng của cloud, được phép điều khiển các ứng dụng triển khai và có thể đồng bộ cài đặt cho môi trường quản lý ứng dụng.
- ***IaaS (Infrastructure as a Service):*** Cung cấp các dịch vụ về hạ tầng, các máy chủ, tài nguyên tính toán (RAM, CPU), lưu trữ. Trên đó người dùng sẽ tạo các máy ảo với hệ điều hành, triển khai ứng dụng theo nhu cầu của mình. (Người dùng không được điều khiển hạ tầng cloud nhưng có thể điều khiển được hệ thống OS, khả năng lưu trữ, và các ứng dụng triển khai, và có thể có một số quyền kiểm soát chọn mạng).

2.2. Tổng quan về công nghệ ảo hóa chức năng mạng – Network Function Virtualization (NFV)

2.2.1. Giới thiệu về công nghệ ảo hóa chức năng mạng

Hiện nay, kiến trúc mạng của các nhà khai thác mạng được phân bổ nhiều thiết bị phần cứng độc quyền. Ứng với mỗi loại dịch vụ, mỗi chức năng mạng lại có các thiết bị phần cứng chuyên trách đảm nhận. Các thiết bị này còn đang có một số hạn chế như: chi phí thiết bị cao, khó quản lý tập trung, độ tương thích thấp với hệ thống của nhiều hãng khác dẫn tới doanh nghiệp phải phụ thuộc vào một số hãng phần cứng nhất định. Để triển khai một dịch vụ mạng mới thường, các nhà khai thác cần giải quyết các bài toán về chi phí năng lượng, chi phí đầu tư vốn và các kĩ năng cần thiết để thiết kế, tích hợp, vận hành và quản lý các thiết bị phần cứng. Không những thế, tuổi thọ của các thiết bị phần cứng đang trở nên ngắn hơn khi đổi mới công nghệ hay dịch vụ tăng tốc, làm ngăn cản việc triển khai các dịch vụ mạng mới và hạn chế cải tiến trong thế giới kết nối mạng ngày càng tập trung như hiện nay.

Công nghệ ảo hóa chức năng mạng - Network Function Virtualization (NFV) ra đời nhằm giải quyết các vấn đề này bằng cách tận dụng công nghệ ảo hóa tiêu chuẩn để hợp nhất nhiều loại thiết bị mạng vào các máy chủ xử lý tốc độ cao, các thiết bị chuyển mạch và thiết bị lưu trữ chuẩn công nghiệp - được đặt tại các trung tâm dữ liệu (Data Center), các điểm chuyển mạch lớn (Network node) trên đường truyền hoặc tại vị trí của người dùng cuối. Nhờ có NFV, các chức năng mạng truyền thống như: NAT, Firewall, Router, IDS, ... tách biệt khỏi các thiết bị vật lý chuyên biệt và được triển khai dưới dạng phần mềm có thể hoạt động trong môi trường ảo hóa trên các thiết bị máy chủ phần cứng phổ thông. Từ đây, việc sử dụng các thiết bị chức năng mạng trở nên linh hoạt hơn: dễ dàng khởi tạo và điều phối các chức năng mạng, giảm thiểu khả năng phụ thuộc vào các nhà cung ứng độc quyền, đồng thời tận dụng nguồn tài nguyên phần cứng hiện có, chi phí vận hành, duy trì và quản lý cũng được giảm thiểu đáng kể.

2.2.2. Lợi ích của công nghệ ảo hóa chức năng mạng

Để thấy rõ được lợi ích của công nghệ ảo hóa chức năng mạng, ta cùng so sánh mô hình mạng truyền thống với mô hình mạng khi áp dụng triển khai NFV thông qua Bảng 2.1 sau:

Bảng 2.1: Bảng so sánh mô hình mạng truyền thống và mô hình mạng ứng dụng NFV

Tiêu chí	Mô hình mạng truyền thống	Mô hình mạng áp dụng NFV
Chi phí thiết bị và chi phí năng lượng	Chi phí cao do phải đầu tư vào nhiều thiết bị phần cứng chuyên biệt, năng lượng tiêu thụ lớn	Chi phí thấp do sử dụng phần mềm, tận dụng được hiệu suất phần cứng phổ thông sẵn có.
Khả năng tùy biến, quản trị, mở rộng và nâng cấp	Khó khăn do phụ thuộc hoàn toàn vào nhà cung cấp thiết bị. Quản lý phân tán gây mất thời gian và công sức của người quản trị. Việc nâng cấp thiết bị gần như là thay thế toàn bộ.	Cao do sử dụng phần mềm hầu như là các giải pháp mã nguồn mở hoặc từ các hãng có cung cấp phần mềm điều khiển. Khả năng mở rộng linh hoạt đáp ứng nhu cầu với các mạng thay đổi thường xuyên. Việc nâng cấp cũng dễ dàng hơn.
Hiệu năng, độ ổn định	Cao do sử dụng các thiết bị phần cứng chuyên biệt cho từng chức năng mạng.	Thấp hơn do ảo hóa trên các thiết bị phần cứng phổ thông. Tuy nhiên, về lâu dài, hiệu năng sẽ dần được cải thiện
Yêu cầu nhân sự	Yêu cầu có kĩ năng sử dụng và vận hành của các hãng thiết bị riêng biệt có trong hạ tầng mạng nhờ tham gia các khóa đào tạo.	Dễ dàng tiếp cận được tài liệu và thông tin để vận hành và quản lý hệ thống mạng. Yêu cầu khả năng cao hơn so với môi trường mạng truyền thống.

Từ bảng trên, ta có thể tóm gọi lại được một số lợi ích tuyệt vời mà công nghệ NFV mang lại như sau: giảm chi phí đầu tư và vận hàng, tận dụng nguồn tài nguyên

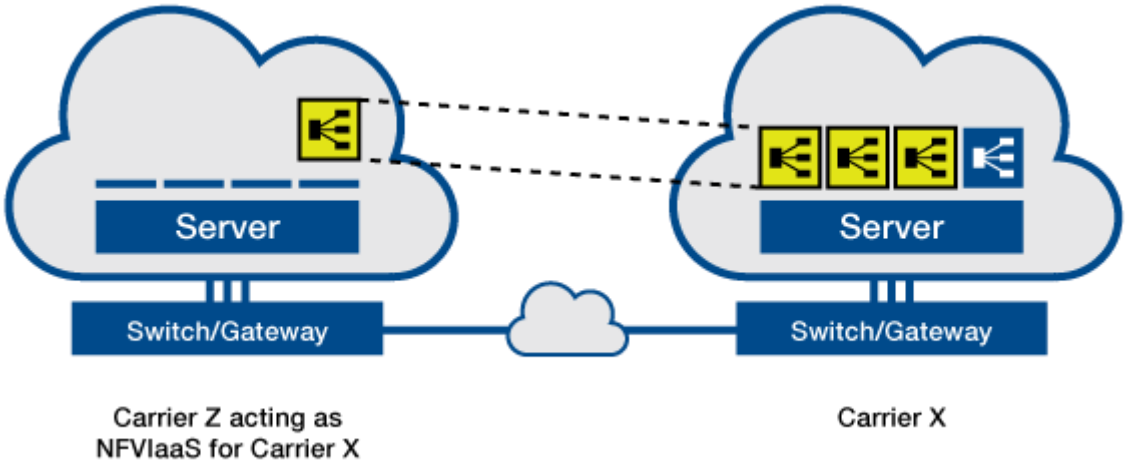
phần cứng sẵn có, cung cấp nhanh chóng và linh hoạt và nhờ giảm bớt thời gian triển khai các dịch vụ mạng mới, các nhà khai thác mạng nắm bắt những cơ hội thị trường mới để tăng lợi nhuận cho doanh nghiệp khi đầu tư vào các dịch vụ mới đó.

2.2.3. Các trường hợp sử dụng của NFV

9 trường hợp sử dụng NFV như sau:

1) Ảo hóa chức năng mạng: Hạ tầng như một dịch vụ

Network Functions Virtualization Infrastructure as a Service: Các nhà cung cấp dịch vụ mạng cung cấp cho các nhà cung cấp khác hoặc khách hàng của họ hạ tầng ảo hóa chức năng mạng của mình để sử dụng lại như một dịch vụ điện toán đám mây theo mô hình IaaS (Infrastructure as a Service).



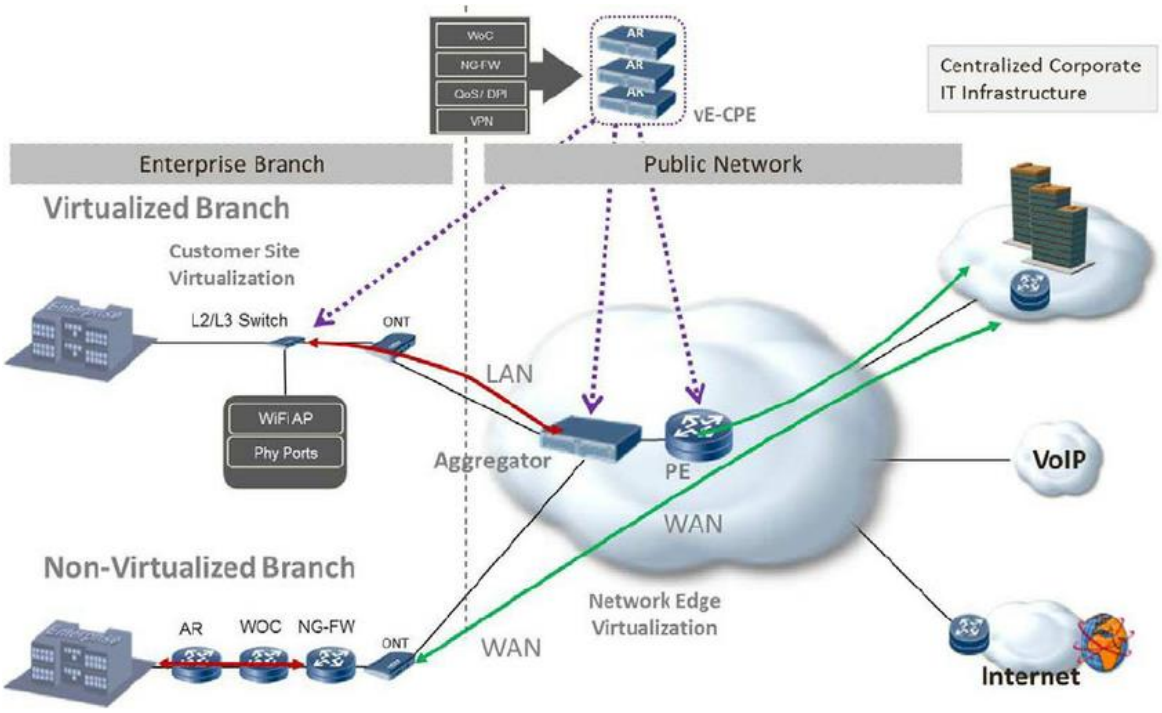
Hình 2.3: Mô hình Ảo hóa chức năng mạng NFVIaaS

Ở Hình 2.3, chức năng mạng ảo hóa bên nhà cung cấp Z được cấp cho bên X sử dụng như cơ sở hạ tầng điện toán đám mây.

2) Ảo hóa chức năng mạng như một dịch vụ (NFV as a Service - NFVaaS)

Các doanh nghiệp hiện nay triển khai nhiều dịch vụ mạng ở các chi nhánh văn phòng khá nhau. Việc đầu tư, vận hành và bảo dưỡng các thiết bị chức năng mạng chuyên dụng truyền thống như: Router, NAT, Firewall, IDS/IPS, ... gây tốn kém khá nhiều chi phí về vật chất và nhân lực. Trong trường hợp này, các nhà cung cấp mạng

viễn thông có thể sử dụng NFV để cung cấp các chức năng mạng CPE (Customer Premises Equipment) dưới dạng điện toán đám mây theo mô hình SaaS (Software as a Service).



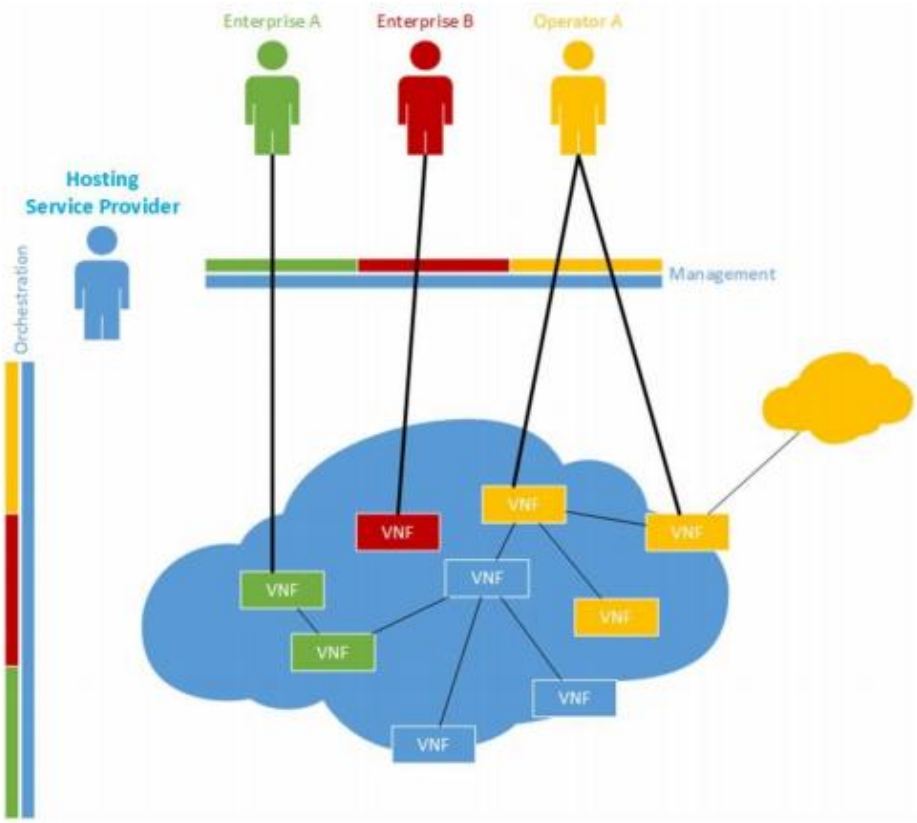
Hình 2.4: Mô hình triển khai CPE truyền thống và vCPE

Như mô tả trên Hình 2.4, lưu lượng truy cập cục bộ của doanh nghiệp được xử lý bởi các thiết bị CPE ảo (vCPE) cung cấp chức năng kết nối lớp 2, lớp 3; và được tích hợp thêm các công nghệ truy cập wifi, hỗ trợ VPN, DPI, WAN Optimazation Controller, QoS. Trong khi triển khai mô hình mạng truyền thống với các thiết bị chuyên dụng, việc vận hành và chi phí thiết bị hẳn sẽ làm đau đầu các chủ doanh nghiệp.

3) Virtual Network Platform as a Service (VNPaaS)

Tài nguyên mạng ngày càng trở nên không bị độc quyền bởi các nhà cung cấp. Các doanh nghiệp hiện nay đã có thể lưu trữ trên cơ sở hạ tầng của nhiều nhà cung cấp. Ảo hóa các chức năng mạng (VNF) làm tăng độ linh hoạt khi chia sẽ các tài nguyên và giảm chi phí thiết lập và quản lý bằng cách cung cấp nền tảng theo mô hình điện toán đám mây PaaS. Các nhà cung cấp có thể đảm bảo độ phù hợp của cơ sở hạ tầng và các ứng dụng như một nền tảng mà trên đó các doanh nghiệp có thể

triển khai các ứng dụng mạng của họ. Với nền tảng này, các doanh nghiệp có thể phát triển tùy ý các dịch vụ mạng theo mục đích kinh doanh của họ.



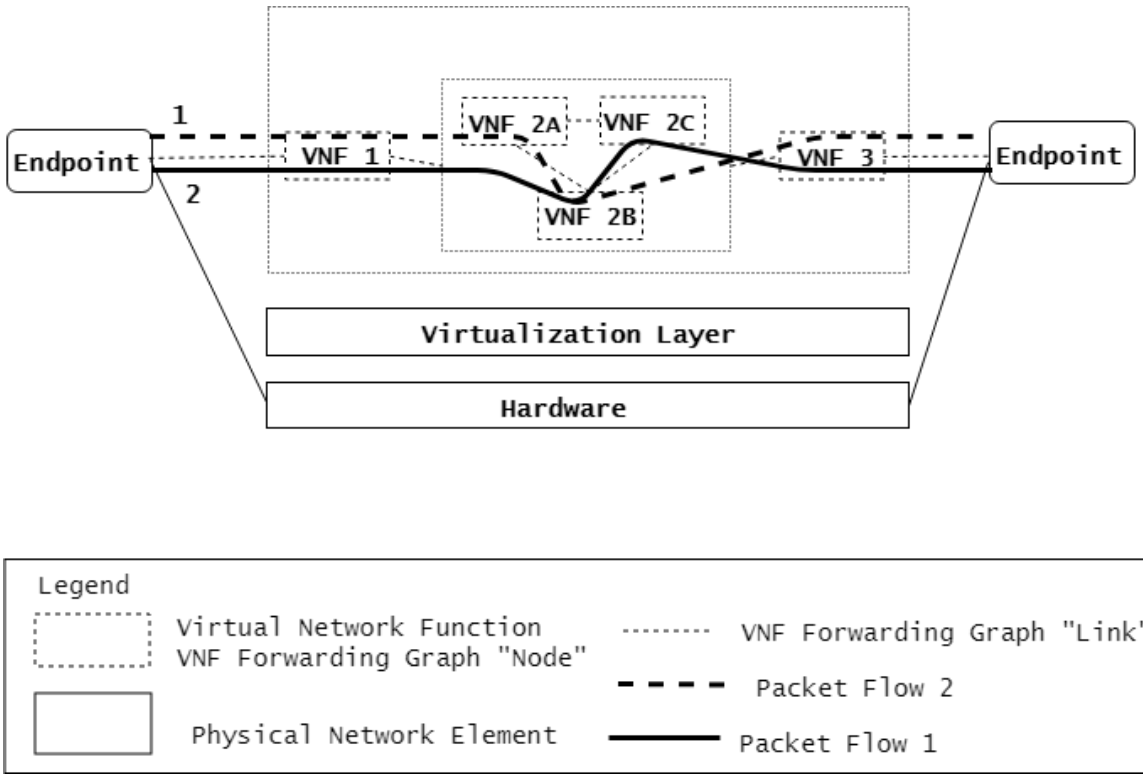
Hình 2.5: Các doanh nghiệp sử dụng chung nền tảng để thực hiện phát triển các dịch vụ mạng của chính mình.

4) Kết nối các chức năng mạng theo mô hình (VNF Forwarding Graphs)

Sử dụng công nghệ ảo hóa chức năng mạng để định nghĩa thứ tự xử lý gói tin theo ý. Một dịch vụ mạng đơn giản có thể được thực hiện trong môi trường NFV sử dụng các liên kết điểm điểm đã định sẵn hướng đi. Để thực hiện được các cấu trúc mạng với lưu lượng đi theo những luồng phức tạp cần tới VNF Forwarding Graph (hay còn gọi là chuỗi các chức năng mạng).

Các đồ hình chuyển tiếp của VNF cung cấp kết nối logic giữa các chức năng mạng ảo, cho phép kích hoạt điều kiển thứ tự di chuyển của luồng lưu lượng giữa các con NFV đó để tạo ra các dịch vụ mạng hoàn chỉnh có quy tắc xử lý lưu lượng tách biệt cụ thể. Ví dụ: trên nền tảng phần cứng vật lý, triển khai NFV ảo hóa các chức

năng mạng và tạo ra hai luồng lưu lượng khác nhau cùng đi qua các con NFV như Hình 2.6:



Hình 2.6: VNF Forwarding Graph

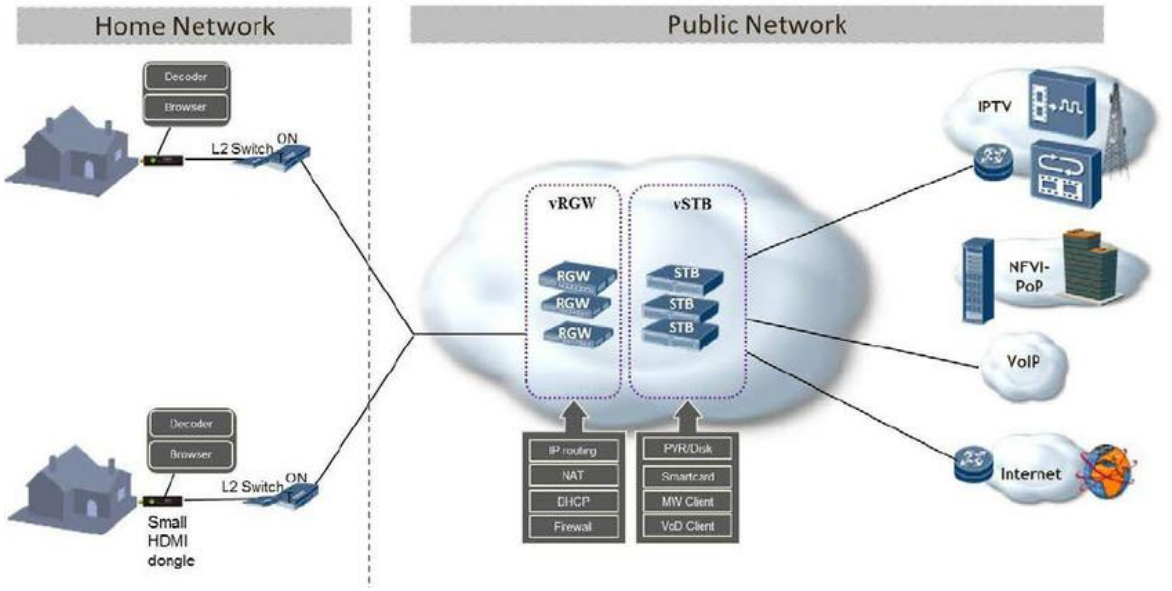
5, 6) Ảo hóa mạng lõi di động, IMS và mạng di động base station:

Trong mạng của các nhà khai thác di động lớn, nhiều node mạng truy cập vô tuyến từ nhiều nhà cung cấp khác nhau thường vận hành trong các kiểu mạng di động khác nhau: 3G, 4G LTE và WiMAX, trong cùng một khu vực. Cho phép các nhà mạng viễn thông, di động ảo hóa hạ tầng triển khai bên dưới để giảm chi phí, tăng hiệu năng và tính sẵn sàng, linh hoạt của hệ thống.

7) Ảo hóa trong môi trường mạng gia đình

Công nghệ NFV trở thành ứng cử viên lý tưởng để hỗ trợ khối công việc tính toán từ các chức năng phân tán trước đây với chi phí tối thiểu và đẩy nhanh thời gian đưa sản phẩm ra thị trường, trong khi các dịch vụ mới có thể được giới thiệu theo yêu cầu ngày càng tăng của khách hàng. Các lợi ích thu được từ việc tránh lắp đặt các thiết bị mới sẽ được nhân lên nếu môi trường mạng gia đình tiếp cận NFV bằng cách thích hợp.

Nhà cung cấp dịch vụ thực hiện ảo hóa một phần hoặc toàn bộ các thiết bị thu nhận/giải mã tín hiệu (Gateway, Modem, Router, ...), các thiết bị CPE chuyên dụng trong mạng gia đình (Setup Box như đầu thu truyền hình Internet). Khách hàng là người dùng cuối trong mạng gia đình không còn cần phải quan tâm tới các bước cấu hình phức tạp cũng như cách thức duy trì và bảo dưỡng các thiết bị đó nữa.



Hình 2.7: Ứng dụng của NFV trong trong môi trường mạng gia đình

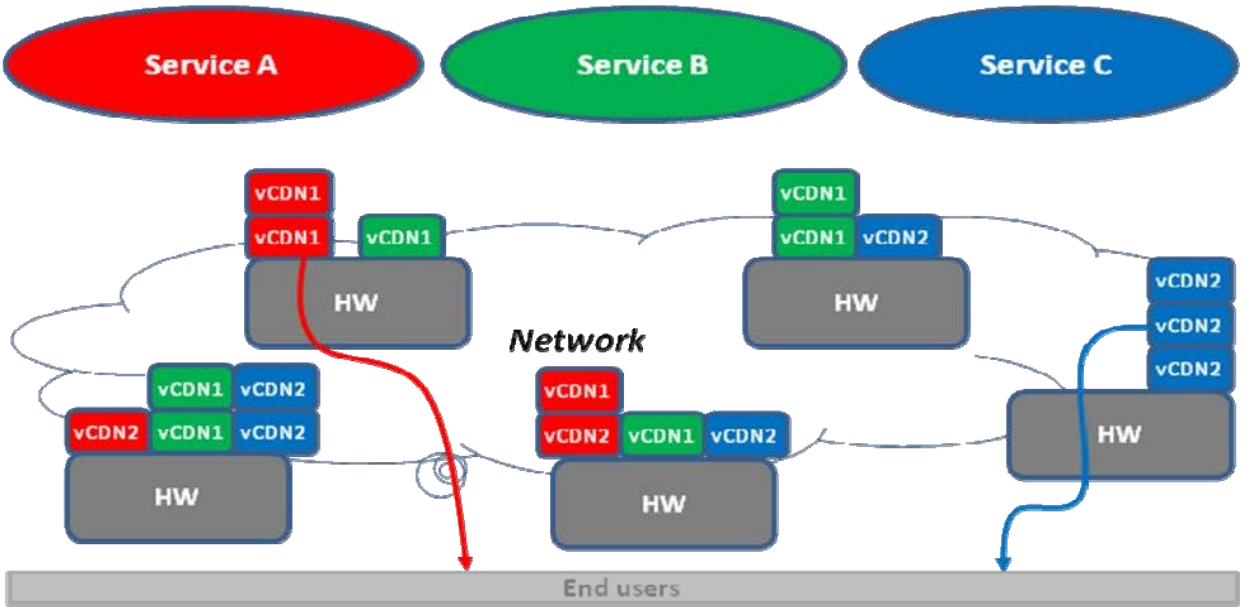
8) Ảo hóa trong mạng CDN (Content Delivery Networks)

Việc cung cấp nội dung dữ liệu, đặc biệt là video - là một trong những thách thức lớn với tất cả các nhà vận hàng mạng do phải phân phối tới khách hàng cuối lưu lượng truy cập ngày càng lớn. Sự gia tăng của lưu lượng vi deo là do sự thay đổi từ phát broadcast sang unicast, do các thiết bị được sử dụng để trình diễn video và bởi cách tăng chất lượng video ở độ phân giải và tốc độ khung hình. Hơn nữa, các yêu cầu về chất lượng cùng đang phát triển: Dịch vụ phát nội dung trực tiếp và phát theo yêu cầu cho người dùng cuối.

CDN là mạng phân phối nội dung hoạt động bởi một bộ điều khiển CDN (CDN controller) tập trung và các nút cache phân tán trong mạng. CDN controller có nhiệm vụ chọn nút cache phù hợp để trả lời request của người dùng, sau đó chuyển hướng request tới nút cache đã chọn. Nút cache sẽ trả lời request của người dùng cuối và cung cấp nội dung được yêu cầu.

Trong các mô hình triển khai hiện nay, các node CDN cache là các thiết bị phần cứng hoặc phần mềm vật lý chuyên dụng với các yêu cầu cụ thể về tiêu chuẩn phần cứng. Thông thường, các thiết bị và máy chủ vật lý cho các mục đích khác nhau được triển khai song song. Việc này dẫn tới nhiều hạn chế.

Việc tích hợp các node trong mạng CDN vào các mạng của nhà vận hành có thể là một cách hiệu quả và tiết kiệm chi phí để giải quyết những thách thức của việc phân phối lưu lượng truy cập video. Triển khai các nút CDN như một phần ảo trong môi trường ảo hóa tiêu chuẩn sẽ giải quyết được hầu hết các thách thức trên.



Hình 2.8: Các nút CDN ảo hóa được triển khai trong một môi trường ảo hóa

9) Ảo hóa các chức năng mạng lớp truy cập cố định - Fixed Access Network Functions Virtualization

Áp dụng NFV sẽ tối ưu tài nguyên kết nối trên các đường truyền cố định lớp Access bằng cách tăng hiệu năng sử dụng, giảm tiêu thụ năng lượng giữa các nút mạng trên đường truyền, tạo ra một nền tảng thống nhất cho các ứng dụng, người dùng và các thuê bao khác nhau. Từ đó, các nhà cung cấp dịch vụ chia sẻ một pool chung quản lý các tài nguyên kết nối và có thể tự động cấp phát và kết hợp các mô

hình triển khai tùy theo yêu cầu dịch vụ khách hàng. Tài nguyên băng thông rộng sẽ được triển khai hiệu quả và sẽ là mô hình kinh doanh mới của các nhà cung cấp.

Hiện nay, tại Việt Nam,việc ứng dụng NFV vào thực tiễn có thể giải quyết các bài toán cụ thể sau:

- Đối với các nhà cung cấp dịch vụ Internet và viễn thông như Viettel, VNPT, FPT, CMC,...
- Ảo hóa hạ tầng mạng Mobile Core Network, IMS và Mobile Base Station kết hợp với công nghệ SDN: triển khai, quản lý các dịch vụ viễn thông di động dễ dàng, nhanh chóng, linh hoạt và tối ưu hơn trên nền hạ tầng phần cứng COTS (Commercial off the Shell).
- Fixed Access Network Functions Virtualization: Tối ưu hóa việc truyền dẫn cũng như cắt giảm chi phí nếu có thể chia sẻ tài nguyên về hạ tầng kết nối với nhau.
- Virtualization of Home Enviroment: quản lý tốt hơn dịch vụ Internet, Thoại, Truyền hình Internet đến người dùng. Cắt giảm chi phí triển khai, bảo trì, sửa chữa, đào tạo con người cho các thiết bị ở tại nhà khách hàng.
- Các công ty kinh doanh nội dung số đa phương tiện như: VNG, FilmPlus, K+,...
- CDN: tối ưu việc xây dựng hạ tầng CDN cho dịch vụ của mình.
- Sử dụng VNF as a Service như: Load balance, Firewall của các nhà cung cấp dịch vụ khác.
- Đối với các công ty cung cấp dịch vụ máy chủ và dịch vụ public cloud như: Vinahost, Vinadata, CMC, vHost,….
- NFVIaaS hoặc Virtual Network Platform as a Service: xây dựng cloud để cho các nhà cung cấp dịch vụ sử dụng để họ tự xây dựng dịch vụ mạng của riêng mình.
- VNF as a Service cung cấp dịch vụ mạng như: Load balance, Firewall,... cho các doanh nghiệp khác.

2.3. Tổng quan về chuỗi chức năng mạng – Service Function Chaining (SFC)

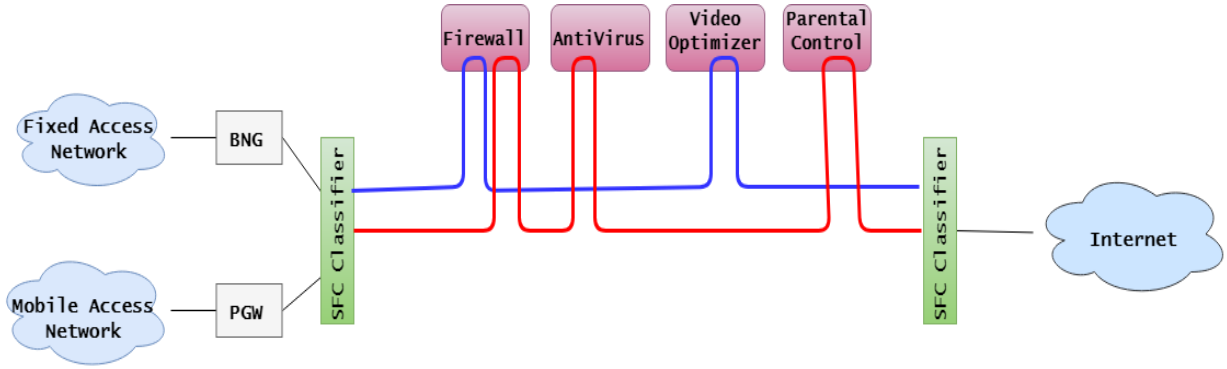
2.3.1. Giới thiệu về chuỗi chức năng mạng

Với sự phát triển nhanh chóng của Internet và các công nghệ như thời điểm hiện nay, việc phát triển thêm các dịch vụ giá trị gia tăng (VAS - Value-Added Services) cho các khách hàng của mình dần trở thành ưu tiên hàng đầu của các nhà cung cấp dịch vụ. Thông thường, luồng lưu lượng được chuyển tiếp thông qua các thành phần mạng đã được nhúng trong các dịch vụ:

- Chuyển hướng trực tiếp một phần lưu lượng tới các thành phần mạng có chức năng giám sát và tính phí.
- Trước khi gửi lưu lượng tới các máy chủ trong trung tâm dữ liệu (DC - Data Center), điều chỉnh lưu lượng đi qua một bộ cân bằng tải để phân phối luồng lưu lượng đi qua nhiều liên kết, qua các chức năng mạng để giảm tải.
- Các nhà vận hành mạng di động chia lưu lượng truy cập băng thông rộng và điều khiển chúng để giảm tải đường xuống.
- Sử dụng chức năng tường lửa để lọc các lưu lượng cho hệ thống IDS/IPS (Intrusion Detection System/Intrusion Protection System).
- Sử dụng các cổng bảo mật để mã hóa và giải mã lưu lượng, có thể kích hoạt các tính năng giảm tải SSL.
- Nếu lưu lượng đến từ các mạng hỗ trợ các địa chỉ khác nhau, ví dụ như IPv4 hoặc IPv6 thì chuyển hướng trực tiếp tới CGN (Carrier Grade NAT) hoặc NAT64.
- Một vài nền tảng dịch vụ nội bộ dựa vào nhận dạng dịch vụ ngầm. Chức năng dịch vụ chuyên dụng được kích hoạt để thêm vào các gói tin (ví dụ: thêm vào HTTP header) với định danh thuê bao hoặc thiết bị người dùng UE (User Equipment).

- Nhà cung cấp cho phép các dịch vụ giá trị gia tăng trên cơ sở từng thuê bao. Mong muốn điều khiển luồng lưu lượng truy cập tới từ các thuê bao đã đăng kí VAS được sử dụng các nền tảng dịch vụ có liên quan.

Chuỗi chức năng dịch vụ (Service Function Chaining - SFC) là công nghệ quy định các chính sách chuyển tiếp lưu lượng tách biệt trong vùng chuỗi dịch vụ. Chuỗi các chức năng dịch vụ mạng SFC định nghĩa và tạo ra một chuỗi các dịch vụ mạng theo thứ tự mong muốn và điều khiển lưu lượng truy cập thông qua chúng.



Hình 2.9: Một chuỗi SFC đơn giản

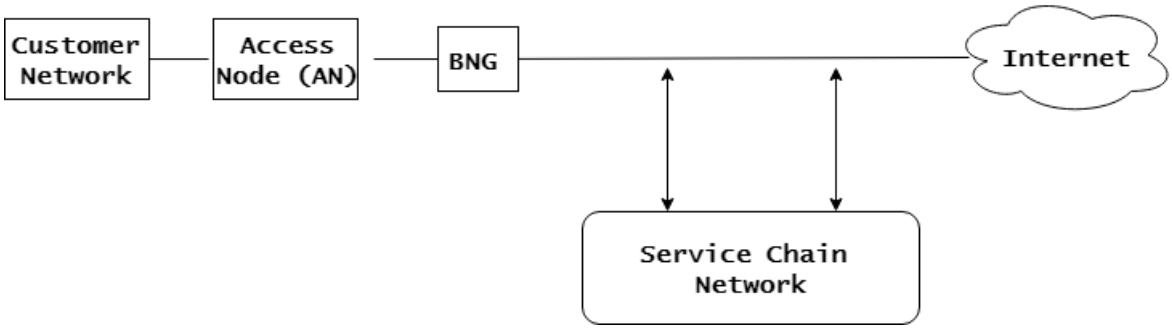
2.3.2. Ứng dụng của SFC trong một số trường hợp cụ thể

Chuỗi chức năng dịch vụ mạng có thể được triển khai trong nhiều mô hình khác nhau như các mạng băng thông rộng (broadband network), các mạng di động (mobile network), và trong các trung tâm dữ liệu (Data Center). Phần này sẽ nêu khái quát một số trường hợp triển khai sử đụng SFC.

1) Ứng dụng SFC vào mạng băng thông rộng cố định (Fixed Broadband Network)

Trong mạng băng thông rộng cố định, người dùng có thể truy cập vào mạng thông qua nhiều công nghệ khác nhau, thường la DSL, Ethernet và PON. Cho dù là bất kì cách thức truy cập nào thì kiến trúc cho phép truy cập và các mạng ngầm tương tự đều gồm các nút truy cập (Access Nodes - ANs) và các Broadband Network Gateway(BNG), trong đó AN thường là các thiết bị cho phép người dùng truy cập

mạng và BNG là nút IP đầu tiên cung cấp khả năng xác thực, ủy quyền và tính toán cho người dùng.



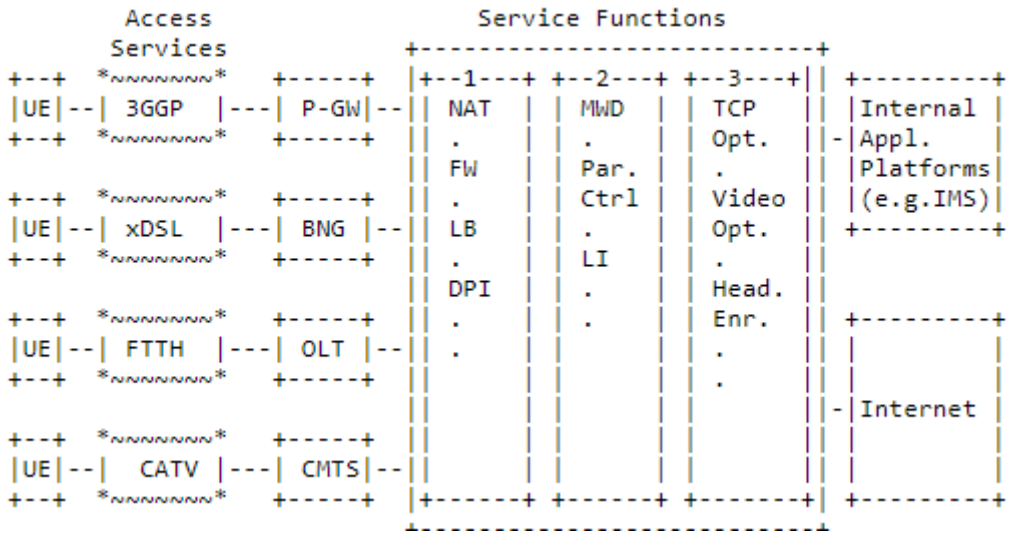
Hình 2.10: Ứng dụng của SFC trong mạng Fixed Boradband Network

Hình 2.10 mô tả mô hình sử dụng SFC trong mạng băng thông rộng cố định. Chuỗi các dịch vụ mạng được triển khai ngay sau BNG và trước khi ra mạng Internet. Chuỗi dịch vụ có thể bao gồm một số dịch vụ như DPI, DS-Lite, Parental control, Firewall, Cân bằng tải (Load banlancer), Cache, ...

2) ứng dụng SFC vào mạng di động

Lưu lượng được chuyển trực tiếp tới/từ Internet đến một hoặc nhiều chức năng dịch vụ mạng. Đó có thể là các chứ năng dịch vụ giá trị gia tăng như dịch vụ kiểm soát (Parental Control) hoặc Tường lửa. Các thuê bao có thể chủ động đăng kí hoặc hủy bỏ các dịch vụ này bất kì lúc nào mà không cần tới sự can thiệp với nhà cung cấp dịch vụ. Một số chức năng dịch vụ cơ bản có thể kể đến như: DPI (Deep Packet

Intrustion), thanh toán và tính phí, tối ưu hóa TCP tối ưu hóa Web, tối ưu hóa video, ...



Hình 2.11: Triển khai SFC trong mạng di động

Hình 2.11 là một ví dụ về triển khai SFC trong các mạng: thiết bị người dùng (User Equitment - UE) truy cập vào mạng di động, luồng lưu lượng được dẫn tới cơ sở hạ tầng có chuỗi các dịch vụ và cuối cùng là kết nối với các nền tảng ứng dụng trên Internet hoặc trong trung tâm dữ liệu riêng của nhà cung cấp. Từ trên xuống dưới có một mạng di động 3GPP kết thúc tại P-GW, một mạng xDSL với đường truyền PPP kết thúc tại BNG, một mạng FTTH và cuối cùng là một mạng truyền hình cab (CATV).

Các chuỗi dịch vụ khác nhau được thực hiện tùy vào nhu cầu của từng loại mạng khác nhau. Chuỗi 1 và 2 có thể áp cho tất cả các mạng trên, nhưng chuỗi 3 với các chức năng tối ưu hóa dữ liệu có thể sẽ chỉ áp dụng với mạng di động.

Các chức năng dịch vụ này có thể đặt trên cùng một thiết bị hoặc đặt trong các hộp độc lập. Để nâng cao chất lượng dịch vụ và trải nghiệm người dùng qua các dịch

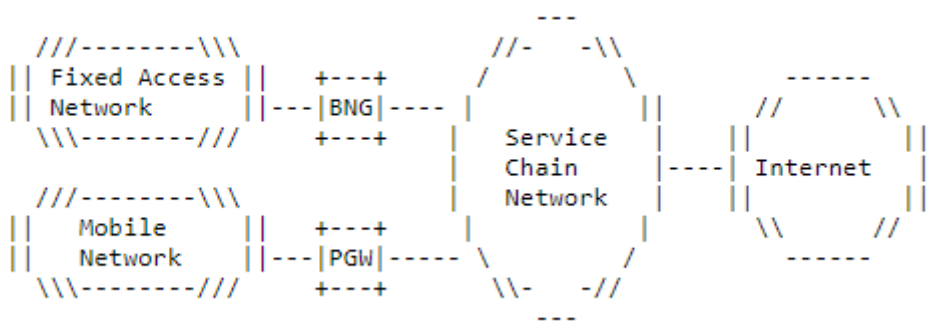
vụ giá trị gia tăng sáng tạo, đáp ứng nhu cầu kinh doanh của các nhà cung cấp, các chức năng dịch vụ ngày càng phát triển.

3) Mạng chuỗi dịch vụ - Công cụ hội tụ mạng

Từ hai trường hợp sử dụng SFC trên, ta có thể thấy sự tương đồng trong chuỗi dịch vụ mạng. Mặc dù mạng băng thông rộng cố định và mạng di động được triển khai tách biệt, với các nhà khai thác tích hợp chạy cả hai mạng này rõ ràng là có lợi khi cung cấp chuỗi dịch vụ dùng chung cho cả hai mạng này.

Ngoài việc tối ưu hóa tài nguyên, một mạng chuỗi các dịch vụ phổ biến có thể cho phép chuyển đổi dịch vụ liền mạch từ mạng này tới mạng khác. Ví dụ: Một khách hàng đang xem trò chơi bóng đá trên điện thoại của mình thông qua mạng di động 4G. Sau khi về nhà, anh ta có thể chuyển qua sử dụng mạng wifi trong nhà của mình - mạng bây giờ chuyển sang mạng cáp quang FTTH (Fiber To The Home) băng thông 100Mbps. Trong trường hợp này, thật dễ dàng khi cung cấp các dịch vụ từ cùng một mạng chuỗi các dịch vụ.

SFC có thể được sử dụng như một công cụ để giải quyết tốt hơn nhu cầu hội tụ.



Hình 2.12: Các mạng dùng chung chuỗi dịch vụ mạng

Hình 2.12 minh họa một mạng chuỗi dịch vụ dùng chung được chia sẻ bởi cả mạng băng rộng cố định và mạng di động. Chuỗi dịch vụ mạng dùng chung có thể được triển khai chỉ bao gồm các nút mạng có chức năng cụ thể hoặc trong trung tâm dữ liệu. Trong cả hai trường hợp, các nút dịch vụ, dù là vật lý hay ảo hóa, đều được chia sẻ bởi cả mạng có dây và mạng không dây. Các nhà khai thác quản lý chuỗi dịch

vụ dùng chung cho cả hai mạng và lưu lượng truy cập từ cả hai mạng có thể đi qua cùng một chuỗi dịch vụ.

4) Chuỗi chức năng dịch vụ phân tán

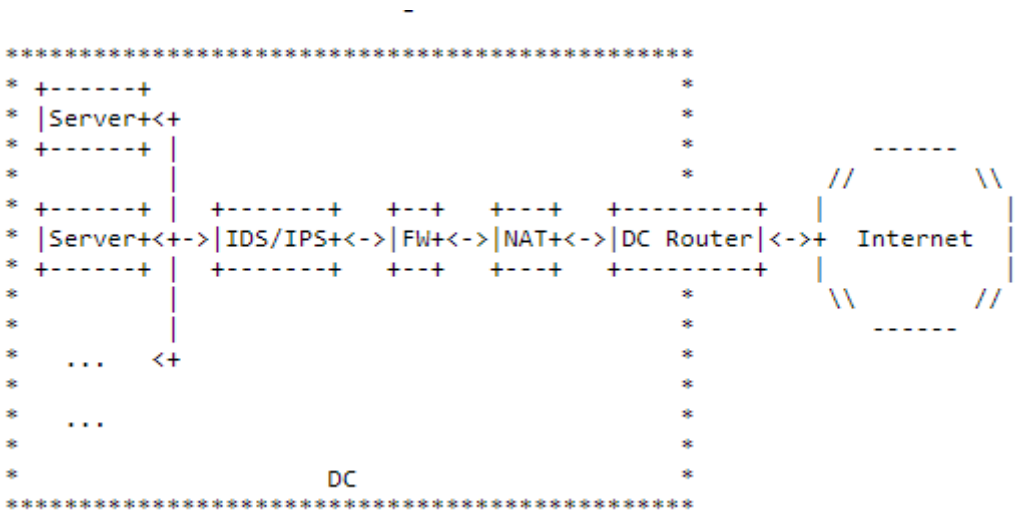
Bên cạnh các trường hợp triển khai kể trên, một chuỗi dịch vụ mạng có thể không cần thiết phải triển khai trong cùng một vị trí mà có thể phân phối qua một số phần của mạng (Data center) hoặc tậm chí sử dụng chức năng dịch vụ đặt gần khách hàng.

Có thể kích hoạt nhiều miền SFC trong cùng một miền quản trị.

5) Triển khai SFC trong trung tâm dữ liệu

Trong trung tâm dữ liệu (DC), như mạng băng rộng và mạng di động, các chuỗi dịch vụ mạng cũng có thể triển khai để cung cấp các dịch vụ giá trị gia tăng.

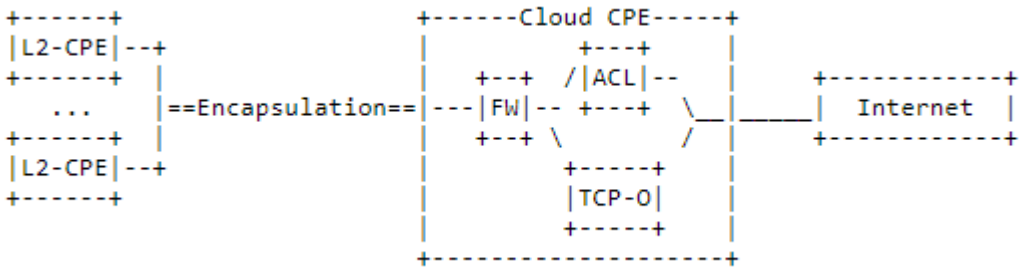
Hình 2.13 mô tả tình huống triển khai SFC trong trung tâm dữ liệu: Các chức năng mạng được đặt giữa router của DC và các máy chủ server. Từ server truy cập ra Internet, có nhiều chức năng dịch vụ như IDS/IPS, Firewall, NAT được sắp xếp tạo thành một SFC nguyên khối xử lý tất cả lưu lượng truy cập tới.



Hình 2.13: SFC trong trung tâm dữ liệu

6) Chuỗi chức năng mạng trong các thiết bị Cloud CPE

Cloud CPE là một kịch bản triển khai mà tập trung vào các dịch vụ giá trị gia tăng (được lưu trữ trong mạng hoặc phía cloud), tách khỏi các hộp dịch vụ phía thuê bao với thiết bị chức năng lớp 2/lớp 3 cơ bản. Trong trường hợp này, tất cả các dịch vụ giá trị gia tăng đều được cấu hình bởi người dùng và được kích hoạt ở phía mạng. Người dùng có thể tự định nghĩa các dịch vụ giá trị gia tăng của riêng họ. Thiết bị Cloud CPE sẽ chuyển các yêu cầu đó thành chuỗi các dịch vụ chức năng. Kiến trúc như vậy phải được hỗ trợ để phân biệt các người dùng khác nhau và lưu lượng của họ.



Hình 2.14: SFC trong các thiết bị Cloud CPE

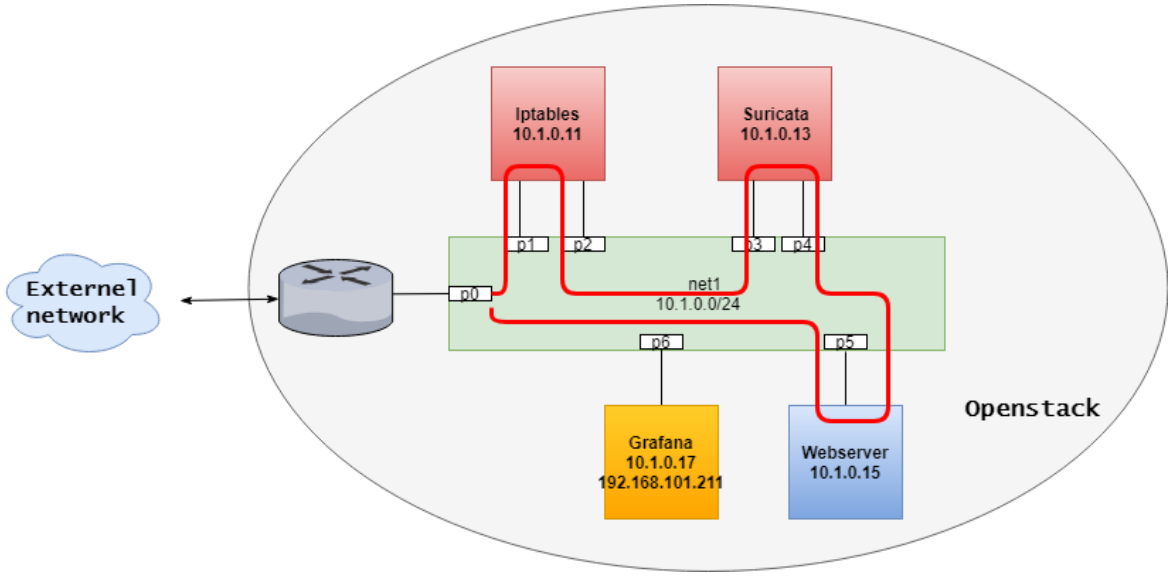
2.4. Kết luận và đưa ra định hướng giải pháp xây dựng đề tài đồ án

Chuỗi chức năng mạng hiện nay phần lớn vẫn sử dụng các thiết bị chuyên dụng, dẫn đến tốn kém về chi phí và phụ thuộc vào nhà sản xuất. NFV ra đời đã giải quyết được vấn đề này bằng việc thay vì phải sử dụng các thiết bị chuyên dụng để làm các chức năng mạng, chúng ta có thể sử dụng các server vật lý được cài các phần mềm giả lập các chức năng mạng như firewall, loadblance,…

Khi NFV kết hợp với SDN sẽ tạo thành chuỗi chức năng mạng SFC linh hoạt, có khả năng quản lý tập trung mạnh mẽ. Qua đó, các nhà mạng có thể tiết kiệm chi phí vận hành, quản lý và cũng bớt lệ thuộc vào các nhà sản xuất thiết bị mạng.

Phần Chương 2 đã trình bày tổng quan về công nghệ ảo hóa chức năng mạng và Chuỗi chức năng mạng, lợi ích cũng như một số trường hợp ứng dụng của hai công nghệ trên. Qua các trường hợp sử dụng NFV và SFC vào hạ tầng mạng đã trình bày ở trên, em lựa chọn xây dựng chuỗi các chức năng mạng ảo hóa bảo vệ các ứng dụng và máy chủ phía nhà cung cấp (hay trung tâm dữ liệu). Chuỗi chức năng mạng sẽ bao gồm 2 thành phần chính là chức năng mạng Firewall có tác dụng chặn, lọc các gói ở lớp 3 và lớp 4; chức năng hệ thống phát hiện xâm nhập NIDS có tác dụng phát hiện các hành vi khả nghi tấn công vào một mạng. Chuỗi chức năng sẽ bảo vệ máy chủ web server bên trong.

3. Chương 3: Xây dựng chuỗi chức năng mạng



Hình 3.1: Mô hình triển khai chuỗi các chức năng mạng ảo hóa

3.1. Xây dựng nền tảng cloud quản lý các chức năng mạng ảo hóa – Openstack

3.1.1. Giới thiệu Openstack

OpenStack là một dự án phần mềm mã nguồn mở dùng để triển khai private và public cloud. Nó bao gồm nhiều thành phần (project) do các công ty, tổ chức và các lập trình viên tự nguyện xây dựng và phát triển.

OpenStack hoạt động theo hướng mở: công khai lộ trình phát triển, công khai mã nguồn mở… OpenStack được phát triển và phát hành phiên bản mới trong vòng 6 tháng, hiện tại đã có 13 phiên bản OpenStack. Tên các phiên bản được đặt theo thứ tự chữ cái A, B, C, … phiên bản hiện tại là Queen. Tới cuối tháng 8/2018, dự định sẽ có phiên bản mới là Rockey.

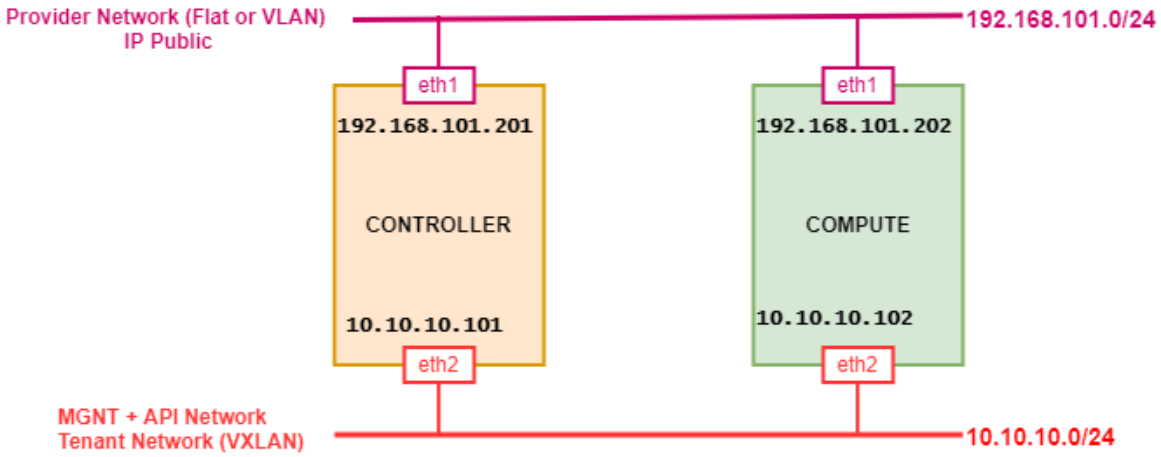
Phần lớn mã nguồn của OpenStack là Python.

Có thể coi OpenStack như một hệ điều hành cloud có nhiệm vụ kiểm soát các tài nguyên tính toán (compute), lưu trữ (storage) và networking trong hệ thống lớn Datacenter, tất cả đều có thể được kiểm soát qua giao diện dòng lệnh hoặc một

dashboard (do project horizon cung cấp). Ở thời điểm hiện tại, OpenStack có 6 core project và 35 project tùy chọn cài đặt theo nhu cầu. 6 core project của OpenStack bao gồm: KEYSTONE, GLANCE, NOVA, NEUTRON, CINDER, HORIZON. 6 project này có nhiệm vụ quan trọng trong việc hình thành nên môi trường cloud và quản lý một cách hiệu quả.

3.1.2. Dựng Openstack để triển khai NFV

Mô hình triển khai Openstack gồm nút chính là Controller và Compute. Đồ hình mức logic như sau:



Hình 3.2: Mô hình triển khai Openstack mức logic

Hệ thống kiểm thử trên mô hình thực tế:

Controller: Là máy chủ server, cài đặt các project: Keystone, Glance, Nova, Neutron, Horizon. Có nhiệm vụ kiểm soát các chức năng chính của Openstack. Khởi tạo và quản lý các tài nguyên trên máy chủ, cho phép tạo các máy ảo đóng vai trò các khối NFV. Yêu cầu tối thiểu 16G RAM, 500G ổ cứng, 8 core CPU.

Compute: là một máy chủ server khác, cài đặt các project Neutron, Nova. Có chức năng cung cấp các tài nguyên tính toán cho các khối chức năng mạng. Yêu cầu tối thiểu 10G RAM, 100G ổ cứng, 10 core CPU.

Về hạ tầng mạng gồm 2 dải như sau:

Dải Provider Network – 192.168.101.0/24: cung cấp kết nối ra mạng bên ngoài cho toàn bộ hệ thống và các chức năng mạng.

Dải MGNT + API network (Management): cung cấp kết nối giữa các khối trong Openstack, quản lý và cấp phát dịch vụ mạng cho các VM bên trong.

2 dải này được cấu hình trên 2 VLAN khác nhau của switch vật lý để tiết kiệm chi phí.

3.2. Xây dựng luồng đi chuỗi chức năng mạng SFC

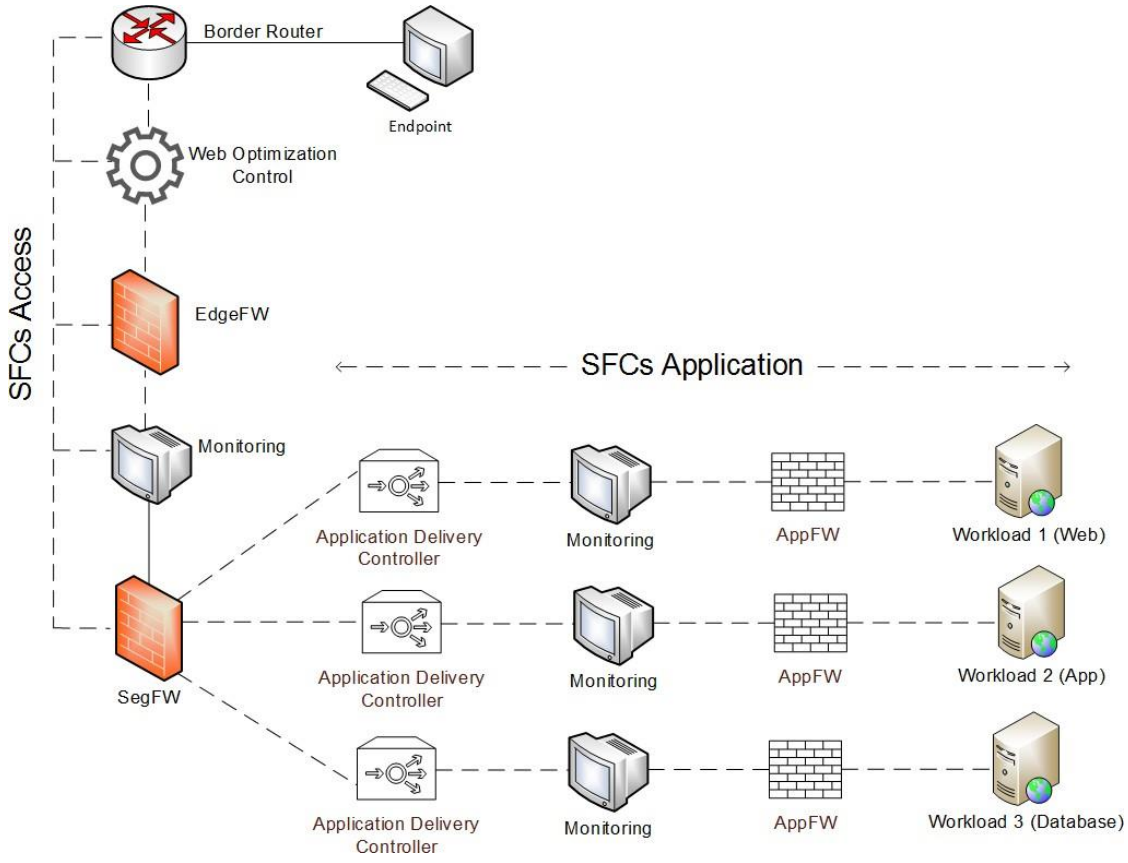
3.2.1. SFC trong trung tâm dữ liệu

Trong trung tâm dữ liệu, nhiều chức năng dịch vụ từ lớp 4 tới lớp 7 được triển khai trên cả thiết bị vật lý và ảo hóa.

Các trung tâm dữ liệu - các doanh nghiệp lớn, cloud hoặc các nhà cung cấp dịch vụ - triển khai các nút dịch vụ tại nhiều điểm khác nhau trong mô hình mạng. Những nút này cung cấp một loạt các chức năng dịch vụ và thiết lập các chức năng dịch vụ được lưu trữ tại một nút nhất định hoặc chống lấp với các chức năng dịch vụ đã được lưu trữ tại các nút dịch vụ khác.

Ứng dụng SFC trong trung tâm dữ liệu gồm ứng dụng cho 3 kiểu lưu lượng sau:

- Lưu lượng từ bên ngoài truy cập vào trung tâm dữ liệu: là các lưu lượng của người dùng cuối truy cập tới dịch vụ của họ trên trung tâm dữ liệu. Đó có thể là lưu lượng truy cập web, đọc tin tức, mạng xã hội và email. Sự gia tăng xu hướng mang mọi thứ tới thiết bị của bạn (Bring Your Own Device - BYOD) và các ứng dụng mạng xã hội yêu cầu lưu lượng phải được phân tích, người dùng phải được xác thực và ủy quyền, nội dung dữ liệu cần được tối ưu hóa để tăng năng suất hoạt động. Ví dụ: lưu lượng từ ngoài vào cần đi qua các chức năng mạng: Firewall, NAT, các chức năng tối ưu hóa nội dung truyền tải, ...
- Lưu lượng truy cập nội bộ trong trung tâm dữ liệu: là loại lưu lượng chính trong trung tâm dữ liệu, kết nối các nút lại với nhau.
- Môi trường đa người dùng: hỗ trợ môi trường nhiều khách hàng là yêu cầu với mọi trung tâm dữ liệu.



Hình 3.3: Chuỗi các chức năng mạng trong trung tâm dữ liệu

3.2.2. Công nghệ xây dựng chuỗi chức năng mạng trên Openstack

Nhắc lại một số kiến thức liên quan OpenStack Networking service (neutron) và OpenStack Compute service, các máy ảo VM kết nối vào một mạng ảo thông qua các port. Điều này cho phép tạo sử dụng mô hình điều khiển lưu lượng đối với SFC sử dụng các port. Việc kết nối các port này trong một chuỗi các port cho phép điều khiển lưu lượng đi qua một hoặc nhiều VM đóng vai trò là chức năng mạng (service function - SF).

Một chuỗi các port tương đương khái niệm Service Function Path (SFP) bao gồm:

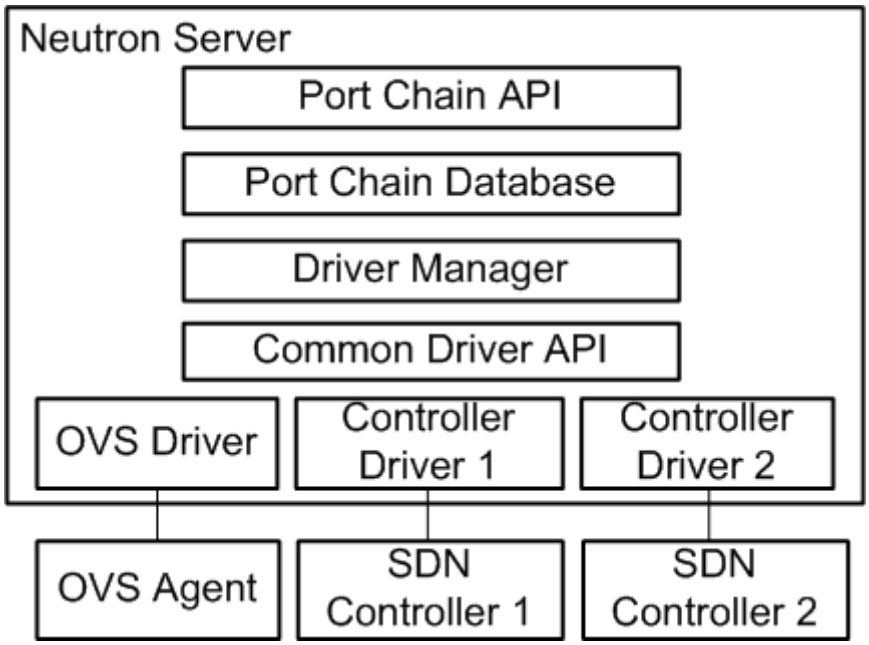
- Một tập các port định nghĩa nên trình tự các chức năng dịch vụ.
- Một tập các flow classifiers (bộ phân loại các luồng) chỉ định các luồng lưu lượng đi vào chuỗi.

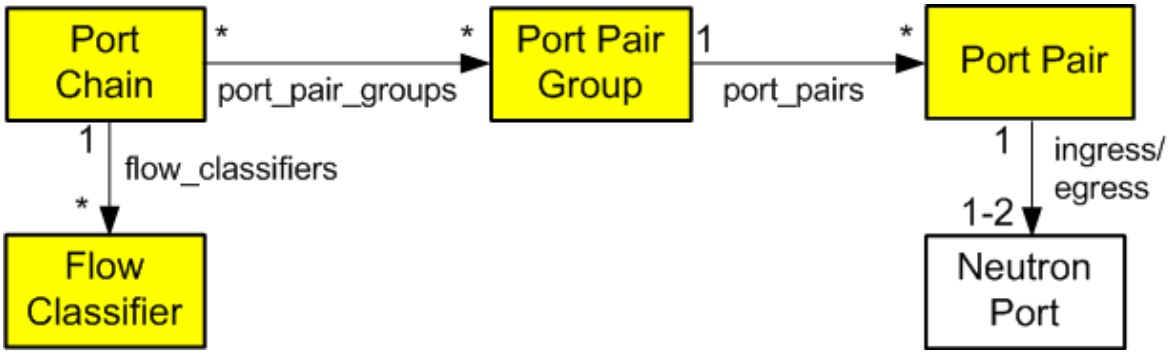
Nếu một SF gắn với một cặp port thì phải chỉ rõ ingress port và exgress port của SF đó. SF cho phép gắn với một port và port đó đóng cả hai vai trò, coi như là một port cho phép lưu lượng đi theo hai chiều vào và ra.

Một chuỗi các port (port chain) được coi là một service chain vô hướng. Một SFC bao gồm hai port chain vô hướng là SFC hai chiều.

Một flow classifier chỉ thuộc về một port chain để tránh việc bối rối khi hệ thống quyết định xem chain nào sẽ xử lý các gói tin. Một port chain có thể gắn với nhiều classifier vì nhiều loại lưu lượng có thể yêu cầu cùng một SFP.

Project networking-sfc là project con của neutron, triển khai port chain plug-in với Open vSwitch driver và SDN Controller drivers (networking-odl hoặc networking-onos) cho phép tương tác với các SFC provider khác nhau (Open vSwitch agent hoặc SDN Controller như OpenDaylight hoặc ONOS). Project này cũng cung cập một driver API chung để hỗ trợ các driver khác nhau đó nhằm cung cấp các giải pháp khác nhau triển khai một SFP.





Hình 3.4: Cấu trúc networking-SFC trong Openstack

3.2.3. Kết quả dựng networking-SFC trên Openstack

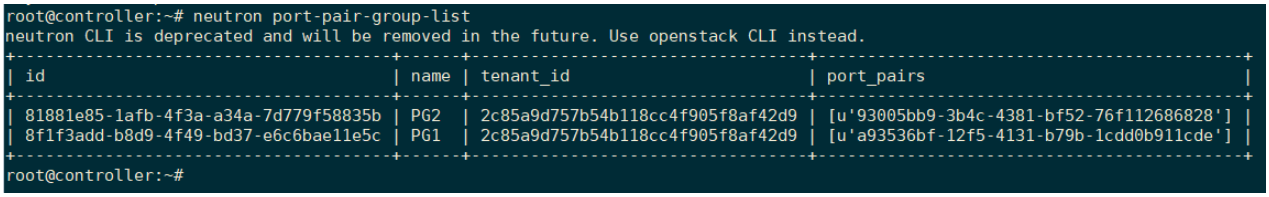
Theo mô hình đã thiết kế, em đã tạo ra trên port chain và port group trên các cổng p1, p2 (nối vào VM Iptables) và p3, p4 (nối vào Suricata). Kết quả như sau:

```
root@controller:~#
root@controller:~# neutron port-pair-list
neutron CLI is deprecated and will be removed in the future. Use openstack CLI instead.
+--------------------------------------+------+----------------------------------+--------------------------------------+--------------------------------------+
| id                                   | name | tenant_id                        | ingress                              | egress                               |
+--------------------------------------+------+----------------------------------+--------------------------------------+--------------------------------------+
| 93005bb9-3b4c-4381-bf52-76f112686828 | PP2  | 2c85a9d757b54b118cc4f905f8af42d9 | 6022be08-3040-4167-af6d-9c077c1818f6 | c6275895-759b-486c-8119-7082cac61184 |
| a93536bf-12f5-4131-b79b-1cdd0b911cde | PP1  | 2c85a9d757b54b118cc4f905f8af42d9 | 4d7a2c9b-e68c-4dea-b701-b5c66e0df1d4 | c7c7effe-9717-470f-9ee8-9f60fdbdc7de |
+--------------------------------------+------+----------------------------------+--------------------------------------+--------------------------------------+
```

Hình 3.5: Kết quả tạo port pair trên các cổng nối với VM

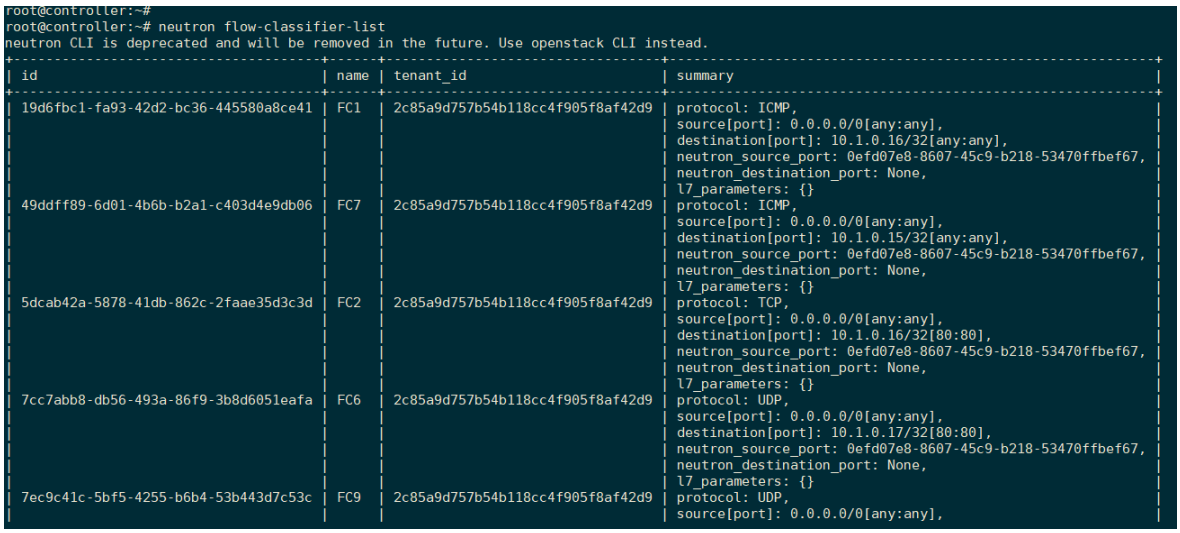
Trong đó, PP1 là port pair nối giữa p1 và p2 của VM Iptables, PP2 và port pair nối giữa cổng p3 và p4 của VM Suricata.

Tạo port pair group chứa các port pair (đại diện cho một hoặc nhiều service function). Nhiều port pair cho phép cân bằng tải hoặc phân bố lưu lượng xử lý trên một tập các service function instance cùng chức năng.



Hình 3.6: Kết quả tạo port-pair-group

Tạo Flow Classifier: Tập hợp các thuộc tính định nghĩa nên flow, gồm cả các thuộc tính về nguồn và đích của flow. Phân biệt giữa các luồng lưu lượng khác nhau sẽ đi qua các chức năng mạng khác nhau.



Hình 3.7: Kết quả tạo Flow Classifier

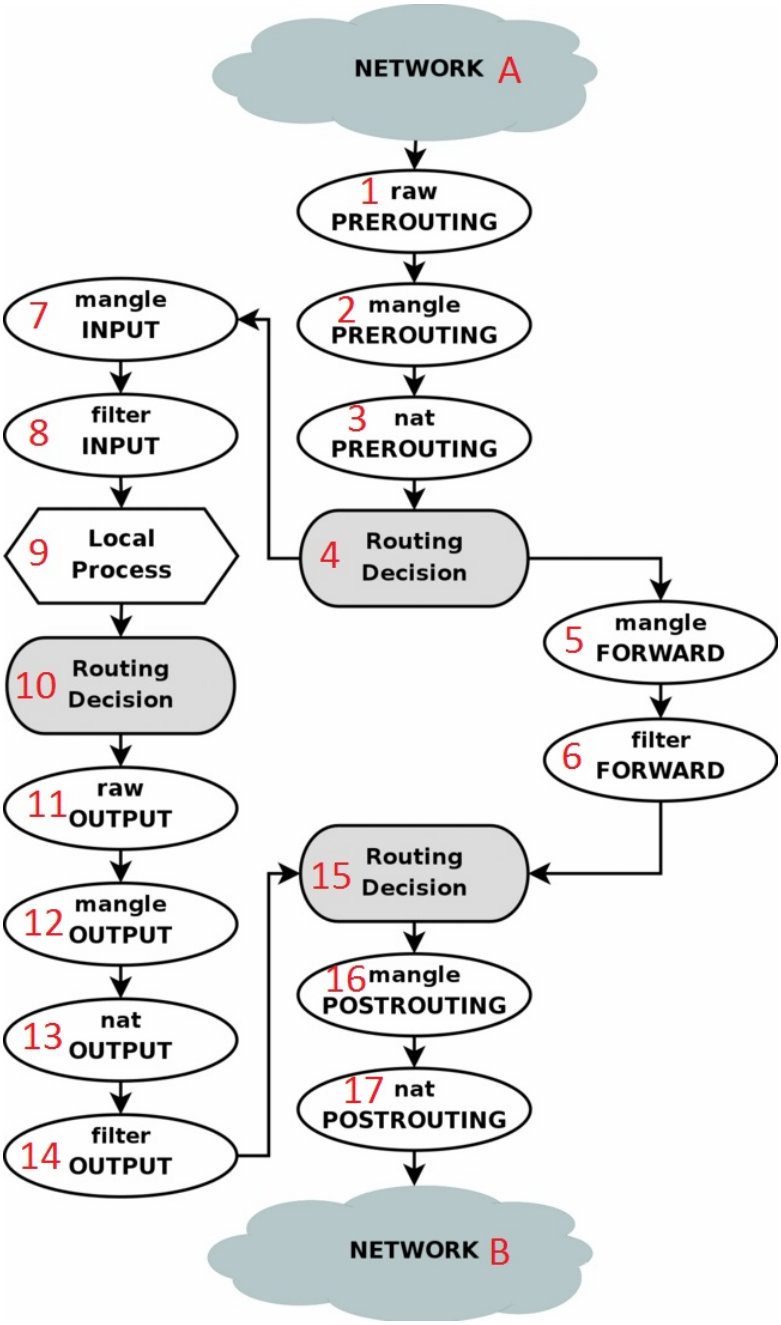
3.3. Xác định các công nghệ sử dụng làm các chức năng mạng

3.3.1. Chức năng mạng Firewall – Iptables

Iptables là một tiện ích firewall cực kì linh hoạt được xây dựng trên các hệ điều hành linux. Iptables là chương trình chạy ở không gian người dùng (user space) cho phép người quản trị hệ thống cấu hình các quy tắc để chặn và lọc gói. Iptables miễn phí và được tích hợp sẵn trong nhân linux.

Iptables thuộc loại firewall có khả năng nhận biết được trạng thái các gói tin này. Từ đó có thể đưa ra quyết định chặn, lọc các gói tin một cách thông minh hơn.

Hơn thế nữa Iptables còn hỗ trợ khả năng giới hạn tốc độ kết nối đối với các kiểu kết nối khác nhau từ bên ngoài, cực kì hữu hiệu để ngăn chặn các kiểu tấn công từ chối phục vụ (DoS) mà hiện nay vẫn là mối đe doạ hàng đầu đối vói các website trên thế giới. Một đặc điểm nổi bật nữa của Iptables là nó hỗ trợ chức năng dò tìm chuỗi tương ứng (string pattern matching), chức năng cho phép phát triển firewall lên một mức cao hơn, có thể đưa ra quyết định loại bỏ hay chấp nhận packet dựa trên việc giám sát nội dung của nó. Chức năng này có thể được xem như là can thiệp được đến mức ứng dụng như HTTP, TELNET, FTP... mặc dù thực sự Netfilter Iptables vẫn chỉ hoạt động ở mức mạng (lớp 3 theo mô hình OSI 7 lớp).



Hình 3.8: Luồng làm việc của IPtables

Quá trình xử lý gói tin của Iptables được mô tả trên Hình 2.3 như sau:

Các gói tin đi từ bên ngoài vào ban đầu được xử lý thông qua chain PREROUTING. Chain này có chức năng thay đổi nguồn của gói tin (nếu cần) trước khi qua các bước xử lý tiếp theo, để hệ thống nhận biết được gói tin có phải dành cho mình hay chuyển tiếp tới các nút mạng tiếp theo.

Sau khi đi qua chain từ PREROUTING, các gói tin được kernel định tuyến. Sẽ có hai trường hợp:

- Nếu gói tin dành cho hệ thống, nó sẽ được đưa tới chain INPUT của bảng mangle và filter để thực hiện các quy tắc trên các bảng đó, cuối cùng được đưa tới tiến trình đảm nhận dịch vụ cho gói tin đó để xử lý.
- Nếu gói tin không dành cho các dịch vụ trên hệ thống, gió tin sẽ được đưa tới chain FORWARD qua các bảng mangle và filter để thực hiện các quy tắc trước khi chuyển tiếp gói tin sang đích chính xác của nó.
- Nếu gói tin được sinh ra từ hệ thống, ban đầu chúng sẽ được định tuyến (bước 10) để xác định được địa chỉ mà nó cần chuyển đến để xác định interface mà gói tin sẽ chuyển ra. Gói tin sau đó được đi qua chain OUTPUT trên các bảng mangle, nat và filter để thực hiện các quy tắc trong các bảng đó.
- Sau cùng, các gói tin được đưa tới chain POSTROUTING (đổi nguồn) và gửi gói tin trở lại mạng.

Trong mô hình SFC em dựng, chức năng mạng Iptables là máy ảo ubuntu server 16.04 có cấu hình 2 core CPU, 2G RAM, 2 card mạng nối vào có địa chỉ trong dải net1 là 10.1.0.11/24 và 10.1.0.12/24.

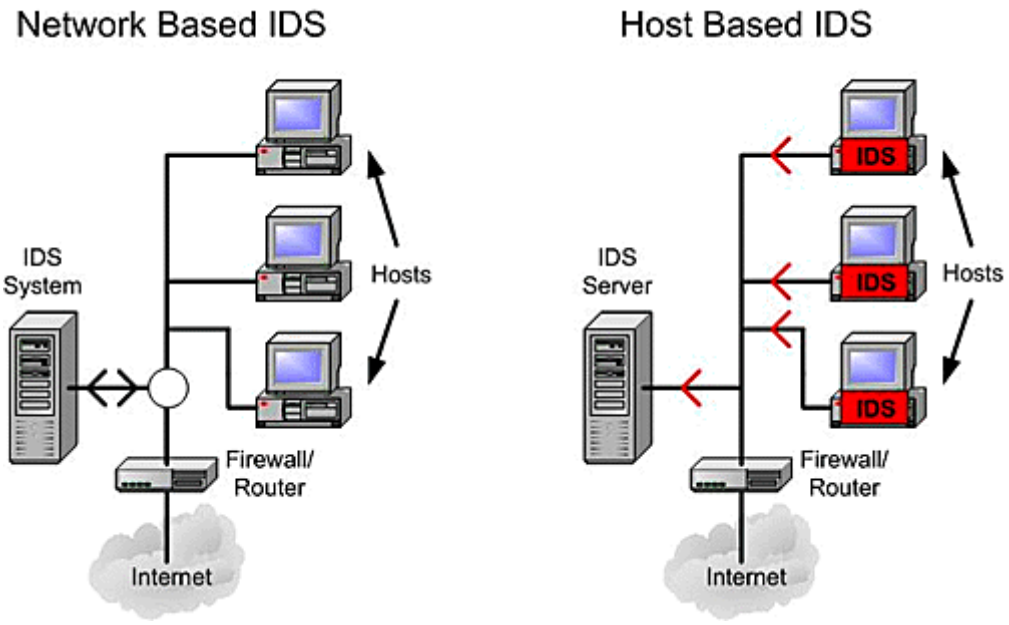
3.3.2. Chức năng mạng Phát hiện xâm nhập (IDS) – Suricata

Ngày nay, khi mạng Internet đã phủ sóng khắp mọi nơi thì thách thức của các vấn đề xâm phạm và tấn công đã khiến các tổ chức phải bổ sung thêm chức năng mạng có tính năng phát hiện và kiểm tra các lỗ hổng bảo mật. Hệ thống phát hiện xâm nhập (IDS) là hệ thống phòng chống có khả năng phát hiện các hành vi khả nghi tấn công vào một mạng. Tính năng chính của hệ thống này là nhận biết những hàng động không bình thường và đưa ra cảnh báo cho người dùng.

Hệ thống IDS phát hiện xâm nhập dựa trên các dấu hiệu đặc biệt về các mối nguy cơ đã biết trước đó trên các gói tin, hoặc so sánh lưu lượng mạng hiện tại với thông số hoạt trong trạng thái bình thường để tìm ra các dấu hiệu bất thường.

Hệ thống IDS được chia thành hai loại cơ bản:

- Network-based IDS (NIDS): sử dụng dữ liệu trên toàn bộ lưu lượng trong mạng để phát hiện bất thường. Kiểu NIDS trong suốt với người dùng cuối, cài đặt và bảo trì đơn giản, không ảnh hưởng tới mạng, có khả năng xác định lỗi ở tầng network và độc lập với hệ điều hành.
- Host based IDS – HIDS: Bằng cách cài đặt phần mềm trên máy chủ, IDS dựa trên máy chủ quan sát tất cả những hoạt động về hệ thống và các file log, lưu lượng mạng thu thập. Hệ thống HIDS theo dõi hệ điều hành, các lời gọi hệ thống và các thông điệp báo lỗi trên máy chủ. HIDS thường được đặt trên một máy tính nhất định thay vì giám sát hoạt động của một mạng, HIDS thường được đặt trên các máy chủ quan trọng và các server trong vùng DMZ.



Hình 3.9: Hai loại hệ thống IDS

Suricata là một công cụ phát hiện mối đe dọa mạng miễn phí, nguồn mở, mạnh mẽ và nhanh chóng.

Suricata có khả năng phát hiện xâm nhập thời gian thực (IDS), phòng chống xâm nhập (IPS), giám sát an ninh mạng (Network Security Monitoring - NSM) và xử lý pcap ngoại tuyến.

Suricata kiểm tra lưu lượng mạng bằng cách sử dụng bộ các quy tắc (rule) xử lý mạnh mẽ và có hỗ trợ kịch bản LUA để phát hiện các mối đe dọa phức tạp. Các rule của Suricata được cập nhật thường xuyên khi phát hiện các

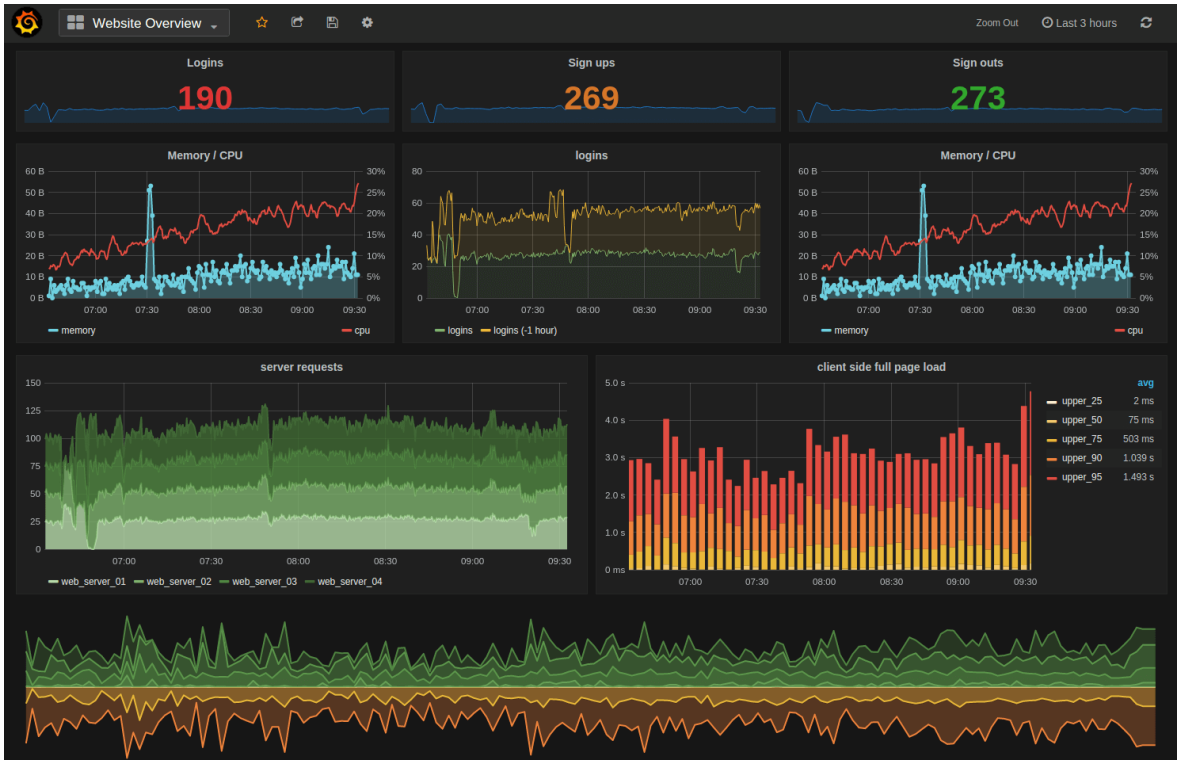
Lý do em lựa chọn Suricata thực hiện chức năng IDS trong mô hình bởi sự phát triển nhanh chóng của Suricata dựa trên cộng đồng và tập trung vào tính bảo mật, khả năng sử dụng và hiệu quả, hỗ trợ đa tiến trình, do đó có thể sử dụng nhiều hơn 1 CPU trong cùng một thời điểm, hỗ trợ trên nhiều nền tảng hệ điều hành như Unix/Linux, FreeBSD và Windows.

Trong mô hình triển khai, chức năng mạng Suricata triển khai trên máy ảo Ubuntu server 16.04, thông số cấu hình 2 core CPU, 2G RAM, 2 card mạng cùng trong dải mạng net1 có IP tương ứng là 10.1.0.13/24 và 10.1.0.14/24. Kích hoạt Suricata hoạt động với 15 000 rule.

3.3.3. Chức năng mạng giám sát – Grafana

Grafana là công cụ được tin tưởng và yêu thích bởi cộng đồng, là nền tảng phân tích tất cả các loại metric.

Grafana cho phép truy vấn, visualize (hiển thị), cảnh báo và giúp người quản trị hiểu metric dù chúng được lưu ở bất kì đâu. Tạo, khám phá và chia sẻ dashboard với nhóm và thúc đẩy văn hóa luồng dữ liệu.



Hình 3.10: Giám sát số liệu hệ thống với Grafana

Các tính năng:

- Visualize (trực quan hóa) : Vẽ biểu đồ từ metric được cung cấp. Grafana có rất nhiều tùy chọn visualize giúp người dùng vẽ biểu đồ một cách nhanh chóng và linh hoạt. Các panel plugin với nhiều cách khác nhau để trực quan hóa các metric và log hệ thống.
- Alerting - Cảnh báo : Giúp người dùng xác định các ngưỡng metric, hiển thị ngưỡng metric cảnh báo và định nghĩa các quy tắc cảnh báo. Grafana liên tục đánh giá metric và gửi cảnh báo khi metric vượt quá ngưỡng cho phép. Cảnh báo có thể được gửi qua Slack, Mail, PagerDuty, Telegram, ...
- Unify – Hợp nhất : Kết hợp dữ liệu để có cái nhìn toàn cảnh tốt hơn. Grafana hỗ trợ hàng chục loại database một cách tự nhiên, kết hợp chúng với nhau trong cùng một giao diện dashboard.

- Open - Mở: Grafana đưa bạn nhiều tùy chọn. Nó hoàn toàn là nguồn mở, được hỗ trợ bởi cộng đồng sôi động. Có thể dễ dàng cài đặt Grafana hoặc sử dụng Hosted Grafana trên bất kì nền tảng nào.
- Extend: Khám phá hàng trăm daaashboard và plugin trong thư viện chính thức. Nhờ đam mê và động lực của cộng đồng, một dashboard hoặc plugin mới được thêm vào mỗi tuần.
- Collaborate - Cộng tác: mang mọi người lại với nhau, chia sẻ dữ liệu và các dashboard với các nhóm. Grafana trao quyền cho người dùng và giúp nuôi dưỡng một nền văn hóa hướng dữ liệu.
- Dynamic Dashboards: Tạo và sử dụng lại các dashboards với các biến template xuất hiện ở phần đầu của dashboard
- Annotations - Chú thích : Biểu đồ chú thích có sự kiện phong phú từ các nguồn dữ liệu khác nhau. Di chuột qua các sự kiện cho bạn thấy siêu dữ liệu sự kiện đầy đủ và các thẻ tag.

Tóm lại: Grafana là công cụ được sử dụng với nhiệm vụ chính là trực quan hóa và phần tích dữ liệu thời gian thực – tức là nó không phải đi thu thập metric từ hệ thống cân giám sát mà chỉ công cụ để hiển thị và phân tích dữ liệu. Với giao diện đẹp mắt và nhiều tính năng tuyệt vời, Grafana được cộng đồng tin tưởng và yêu thích sử dụng. Có hơn 150000 hệ thống grafana đang hoạt động trên toàn thế giới với nhiều usecase sử dụng phong phú.

Với những lợi ích như trên, em chọn Grafana làm chức năng giám sát các thông số trong mạng. Grafana sẽ biểu thị thông tin về metric được thu thập bởi Collectd được cài trên các chức năng mạng Iptables và Suricata. Trong mô hình triển khai, Grafana là VM Ubuntu Server 16.04 có thông số cấu hình 1 core CPU, 1G RAM, có một card mạng trong dải net1 để nhận metric chuyển về từ các VM khác trong mạng, có IP 10.1.0.19/24.

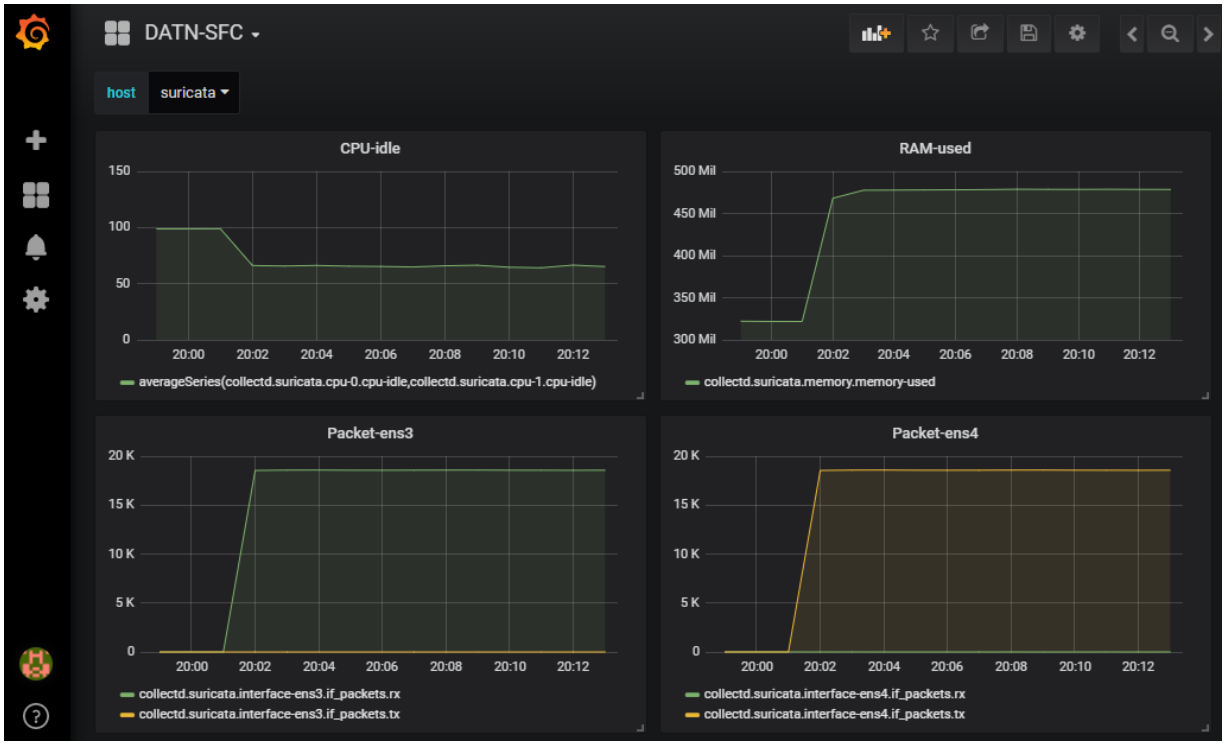
4. KẾT QUẢ ĐO ĐẠC VÀ ĐÁNH GIÁ

4.1. Kiểm chứng luồng lưu lượng đi theo đúng mô hình SFC đã dựng

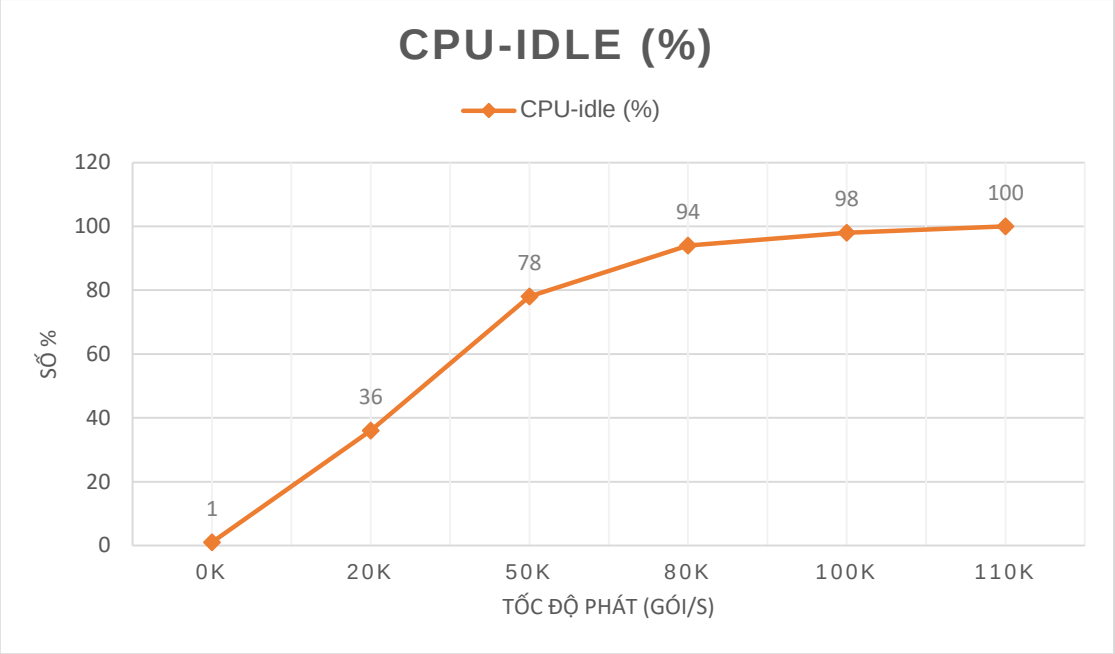
Để kiểm chứng lưu lượng đã đi qua các chức năng mạng Iptables, Suricata rồi mới tới Web server. Từ bên ngoài, thực hiện ping vào thấy lưu lượng đi qua Iptables và Suricata như sau:

4.2. Kết quả đo lượng tài nguyên sử dụng trên Suricata

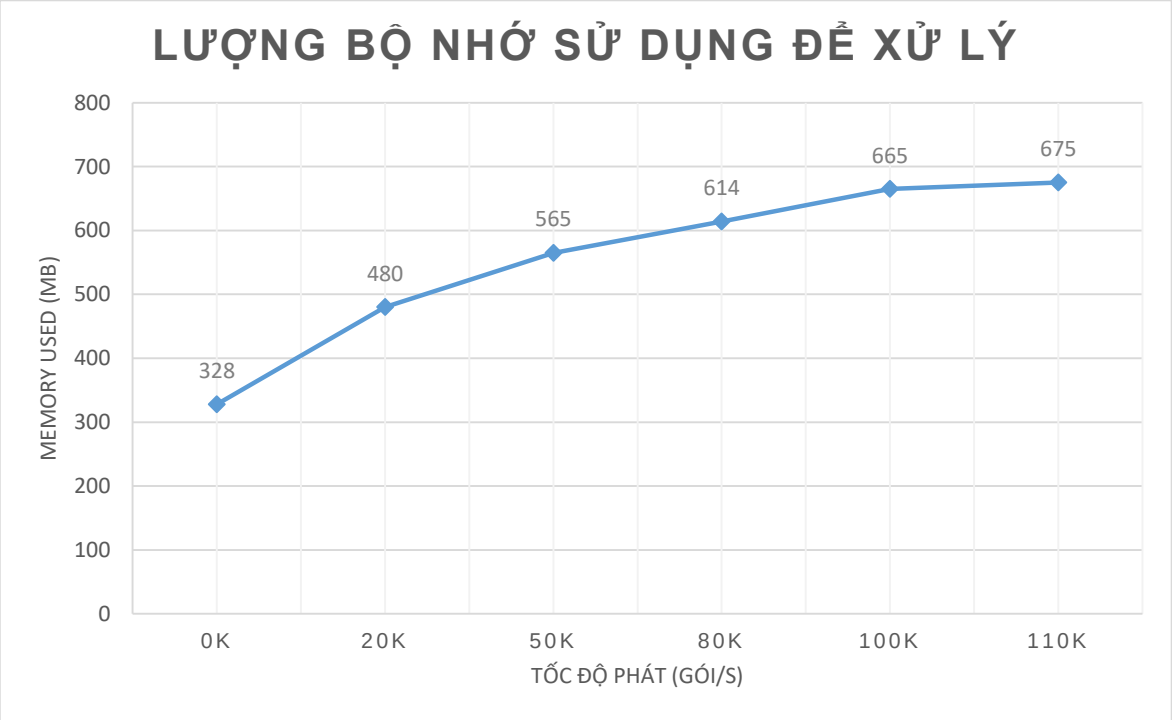
Sau khi xây dựng mô hình, thực hiện đo đạc các thông số sử dụng về CPU và memory trên chức năng mạng Suricata.



Hình 4.1: Theo dõi thông số tài nguyên sử dụng trên Suricata



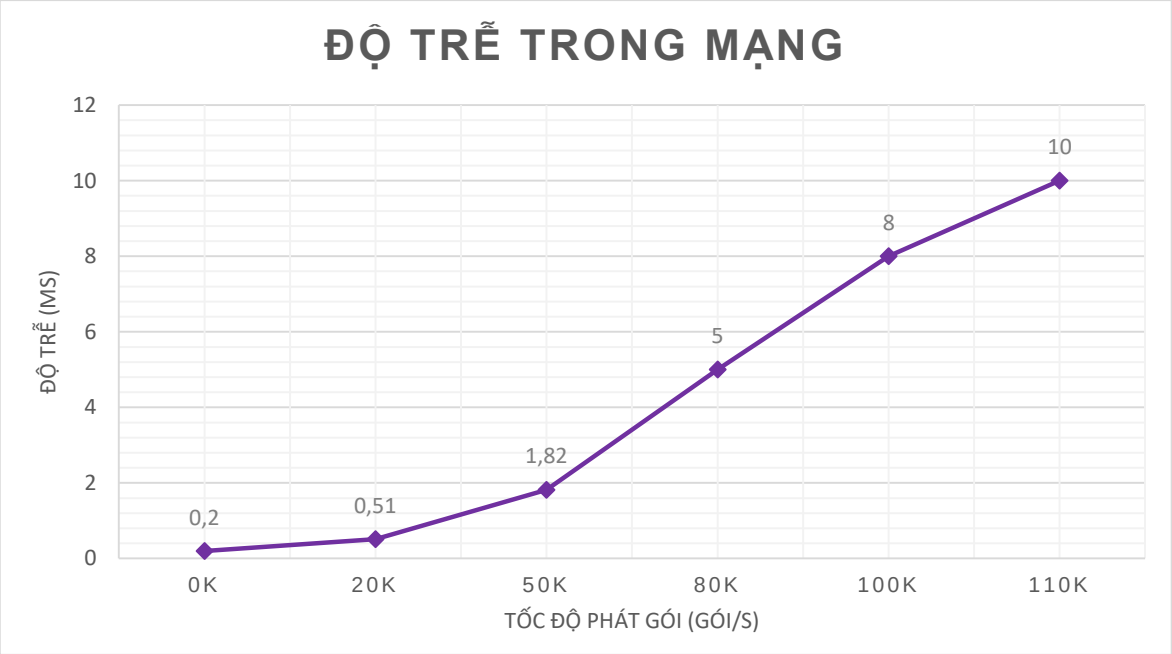
Hình 4.2: Kết quả sử dụng CPU trên Suricata



Hình 4.3: Lượng bộ nhớ sử dụng để xử lý các gói tin trên Suricata

4.3. Kết quả đo độ trễ của lưu lượng khi đi qua chuỗi các chức năng mạng

Phát lần lượt số lượng các gói tin TCP tăng dần vào chuỗi SFC. Thực hiện kích hoạt plugin ping (của collectd) trên máy client từ bên ngoài mạng. Cấu hình client cứ mỗi giây ping tới web sererver một lần để đo thông số thời gian round trip time của gói tin trả về. Độ trễ gói tin trả về tăng dần khi tải hệ thống tăng dần như sau:



Hình 4.4: Kết quả đo độ trễ trong mạng

4.4. Đánh giá kết quả

5. KẾT LUẬN

6. TÀI LIỆU THAM KHẢO