STT	Người ký	Đơn vị	Thời gian ký	Ý kiến
1	Hoàng Sinh Trường	Giám đốc - Trung tâm Dịch vụ số MobiFone	08/11/2022 15:02:25	-
2	Nguyễn Việt Hùng	Trưởng phòng - Phòng Kỹ thuật khai thác	08/11/2022 10:05:54	Kính trình

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

TRUNG TÂM DỊCH VỤ SỐ MOBIFONE

Số: 372/QĐ-TT.MDS

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập-Tự do-Hạnh phúc

Hà Nội, ngày 8 tháng 11 năm 2022

QUYẾT ĐỊNH

Về việc ban hành Quy trình Quản lý vận hành khai thác các hệ thống mạng và bảo mật

GIÁM ĐỐC TRUNG TÂM DỊCH VỤ SỐ MOBIFONE

Căn cứ quyết định số 216/QĐ-MOBIFONE ngày 01/02/2019 của Tổng Giám đốc Tổng Công ty Viễn thông MobiFone về việc sáp nhập, đổi tên và điều chỉnh nhiệm vụ chính của các đơn vị thuộc Trung tâm Dịch vụ đa phương tiện và giá trị gia tăng MobiFone.

Căn cứ quyết định số 238/QĐ-HĐTV ngày 03/02/2021 của Hội đồng thành viên Tổng Công ty Viễn thông MobiFone về việc thay đổi tên của Trung tâm Dịch vụ Đa phương tiện và Giá trị gia tăng MobiFone.

Căn cứ vào nhu cầu, tình hình thực tế về quản lý vận hành khai thác các hệ thống dịch vụ số MobiFone.

Theo đề nghị của Trưởng phòng Kỹ thuật khai thác.

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này "Quy trình Quản lý vận hành khai thác các hệ thống mạng và bảo mật".

Điều 2. Quy trình có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 3. Các Ông (Bà) Phó Giám đốc Trung tâm; Trưởng các Phòng chức năng, đơn vị trực thuộc Trung tâm và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận **:**
- Như điều 3 (để t/h);
- Lưu: VT, KTKT.

GIÁM ĐỐC

TRUNG TÂM DỊCH VỤ SỐ MOBIFONE - CHI NHÁNH TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

Hoàng Sinh Trường

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE
TRUNG TÂM DỊCH VỤ SỐ MOBIFONE

QUY TRÌNH QUẢN LÝ VẬN HÀNH KHAI THÁC CÁC HỆ THỐNG MẠNG VÀ BẢO MẬT

(ban hành kèm Quyết định số 372/QĐ-TT.MDS ngày 08/11/2022 của Trung tâm Dịch vụ số MobiFone)

Ban hành lần 4
Lưu hành nội bộ

Hà Nội, 11/2022

QUY TRÌNH QUẢN LÝ VẬN HÀNH KHAI THÁC CÁC HỆ THỐNG MẠNG VÀ BẢO MẬT

NGƯỜI ĐƯỢC PHÂN PHÁT:

1. Ban Giám đốc Trung tâm dịch vụ Số MobiFone;
2. Trưởng phòng Kỹ thuật Khai thác;
3. Trưởng phòng Phát triển Dịch vụ;
4. Giám đốc Chi nhánh Hồ Chí Minh.

NGƯỜI VIẾT:

Họ tên	Chức vụ	Ký
NguyễnViệt Hùng	**Trưởng phòng Kỹ thuật Khai thác**	

NGƯỜI DUYỆT:

Họ tên	Chức vụ	Ký
Hoàng Sinh Trường	**Giám Đốc Trung tâm Dịch vụ Số MobiFone**	

TÓM TẮT SỬA ĐỔI			
Lần sửa	**Ngày sửa**	**Người duyệt**	**Tóm tắt nội dung sửa đổi**
	30/09/2016	Nguyễn Tuấn Huy – Giám đốc Trung tâm	-
1	30/03/2021	Hoàng Sinh Trường – Giám đốc Trung tâm	- Theo QĐ 216/QĐ-MOBIBONF ngày 01/02/2019 về việc "Sát nhập, đổi tên và điều chỉnh nhiệm vụ của các đơn vị thuộc Trung tâm Dịch vụ Đa phương tiện và Giá trị gia tăng MobiFone", Chi nhánh Hồ Chí Minh sẽ không còn nhiệm vụ quản lý vận hành khai thác các hệ thống, dịch vụ giá trị gia tăng và QĐ số 238/QĐ-HĐTV ngày 03/02/2021 của Hội đồng thành viên Tổng Công ty Viễn thông MobiFone về việc "Thay đổi tên của Trung tâm Dịch vụ Đa phương tiện và giá trị gia tăng MobiFone".
			- Cập nhật tại danh mục thiết bị của các đơn vị theo nhiệm vụ vận hành, khai thác mới.
			- Thay đổi phương thức quản lý tại các site. Phòng Kỹ thuật Khai thác quản lý toàn bộ Mạng Tin học tại Trung tâm: bao gồm các site Yên Hòa, Giáp Bát, Đà Nẵng và Hồ Chí Minh (quản lý khai thác và điều hành hoạt động mạng tại Hồ Chí Minh. Chi nhánh Hồ Chí Minh phối hợp quản lý hạ tầng, nguồn điện và các thiết bị accesss).
2	27/10/2021	Hoàng Sinh Trường – Giám đốc Trung tâm	- Cập nhật quy trình cấp phát, thu hồi địa chỉ IP, quy trình khai báo kết nối trên các thiết bị Firewall. Cập nhật Phiếu đề nghị cấp phát/thu hồi địa chỉ IP.

3	01/11/2022	Hoàng Sinh Trường – Giám đốc Trung tâm	- Cập nhật sơ đồ kết nối mạng tin học trung tâm tại site Yên Hòa, Hồ Chí Minh. - Cập nhật danh sách thiết bị Firewall Fortigate, Router CP 7613. - Cập nhật thông tin lưu nhật ký thiết bị mạng và bảo mật. - Cập nhật quy trình khai báo rule Firewall cho các hệ thống Fintech, Mobile Money, dịch vụ ứng và các hệ thống thông tin cấp độ 3.

MỤC LỤC

CÁC TỪ VIẾT TẮT

Chữ viết tắt	Ý nghĩa
CNHCM	Chi nhánh Hồ Chí Minh
DB	Database
ĐHKT	Điều hành kỹ thuật
ĐPT	Đa phương tiện
FTP	File Transfer Protocol
GTGT	Giá trị gia tăng
KTKT	Kỹ thuật Khai thác
MDS	MobiFone Digital Service Central
OMC	Operating Management Center
PTDV	Phát triển dịch vụ
QoS	Quality of Service
SMS	Short Message service
SNMP	Simple Network Management Protocol
VHKT	Vận hành khai thác

A. NHỮNG QUY ĐỊNH CHUNG

I. MỤC ĐÍCH:

- Quy trình này nhằm đưa ra những quy định, thủ tục vận hành khai thác các hệ thống thiết bị mạng và bảo mật do Trung tâm Dịch vụ Số MobiFone quản lý.
- Các quy trình này được các cán bộ kỹ thuật thực hiện theo chức năng, nhiệm vụ. Không tuỳ tiện thực hiện khi không có nhiệm vụ.

II. CÁC VĂN BẢN CÓ LIÊN QUAN:

- Quy trình quản lý chất lượng dịch vụ (ban hành kèm theo văn bản 348/QĐ-MVAS-DVGTGT ngày 18/09/2015);
- Quy định bảo dưỡng, sửa chữa thiết bị mạng, dịch vụ thông tin di động MobiFone theo văn bản 998/QĐ-MOBIFONE-QLĐHM ngày 02/06/2015;
- Quy định quản lý thiết bị tin học của Tổng Công ty Viễn thông MobiFone theo văn bản số 1635/QĐ-MOBIFONE ngày 27/08/2018;
- Quy định quản lý và sử dụng địa chỉ IP của Tổng Công ty Viễn thông MobiFone theo văn bản số 793/QĐ-MOBIFONE ngày 12/04/2018;
- Căn cứ các quy trình, quy định hiện hành.

III. PHẠM VI ÁP DỤNG:

- Quy trình này áp dụng tại các đơn vị liên quan trong nội bộ Trung tâm Dịch vụ Số MobiFone trong việc khai thác vận hành các hệ thống thiết bị mạng và bảo mật.
- Phân công nhiệm vụ vận hành khai thác.
- Các thiết bị mạng và bảo mật do Phòng Kỹ thuật Khai thác quản lý vận hành.
- Các thiết bị mạng và bảo mật các hệ thống do Chi nhánh Hồ Chí Minh quản lý vận hành.

IV. YÊU CẦU CHUNG:

- Người thực hiện các quy trình này phải là các cán bộ kỹ thuật đã qua đào tạo, phải nắm vững cấu hình phần cứng cũng như các lệnh thao tác.
- Trước khi thực hiện quy trình cần nắm rõ cấu hình cụ thể của hệ thống mạng và các đặc điểm riêng biệt của thiết bị.
- Khi thực hiện quy trình phải tuyệt đối tuân thủ theo các quy định về an toàn thông tin, an toàn hệ thống, an toàn vận hành khai thác cho người và thiết bị, an toàn

về điện và phòng chống cháy nổ.

- Trước khi thực hiện các công việc về thay thế phần cứng cần kiểm tra chặt chẽ các yêu cầu về vị trí, nguồn điện, phần mềm, phần cứng và sự tương thích, phù hợp của các thông số cấu hình.
- Trong quá trình khai thác, vận hành và bảo dưỡng hệ thống phải đảm bảo an toàn cho hệ thống mạng, hệ thống dịch vụ giá trị gia tăng.
- Các nhân viên quản lý khai thác, vận hành và bảo dưỡng hệ thống phải tuân thủ các bước và các quy định trong quy trình này.
- Không sử dụng máy tính dùng cho các hệ thống thiết bị mạng và bảo mật vào mục đích riêng.
- Tuân thủ các quy định về phòng chống virus khi vận hành, khai thác hệ thống.
- Lưu trữ các thiết bị dự phòng đúng nơi quy định, đảm bảo thay thế khi cần thiết.
- Trước khi thực hiện các quy trình vận hành, khai thác, bảo dưỡng cần phải thông báo và được sự chấp thuận của người chịu trách nhiệm của hệ thống.
- Kết quả thực hiện quy trình phải ghi chép sổ sách đầy đủ.
- Nhân viên khai thác, vận hành phải đảm bảo giữ an toàn, bí mật về tài khoản, mật khẩu của hệ thống. Tuyệt đối không được để lộ thông tin cho người không có trách nhiệm dùng để đăng nhập vào hệ thống.
- Bản quy trình này đưa ra những quy trình cơ bản, tuy nhiên trong quá trình vận hành khai thác, bảo trì bảo dưỡng có thể xuất hiện những lỗi đặc biệt khác sau khi sử dụng quy trình này mà vẫn chưa xử lý được cần phải báo cáo với người chịu trách nhiệm kỹ thuật của hệ thống hay của các cấp Lãnh đạo cao hơn để tìm biện pháp xử lý.
- Trong quá trình xử lý sự cố, khai thác bảo dưỡng cần tuân thủ theo các Quy trình được nêu tại mục các văn bản có liên quan (mục A của Quy trình này) và các quy định về yêu cầu hỗ trợ kỹ thuật từ đối tác do Tổng Công ty và Trung tâm Dịch vụ Số MobiFone quy định.

V. QUY ĐỊNH CHUNG VỀ THỜI GIAN VÀ NGƯỜI THỰC HIỆN

Đối với công việc thực hiện hàng ngày:

- Thời gian thực hiện: trong giờ hành chính.
- Người thực hiện: nhân viên chuyên trách quản lý hệ thống.

Đối với công việc thực hiện hàng tuần

- Thời gian thực hiện: thực hiện vào Thứ 6 hàng tuần (thời gian thực hiện tùy theo từng công việc và tuân thủ theo quy định cụ thể ghi trong phần thủ tục thực hiện của công việc).
- Người thực hiện: nhân viên chuyên trách về hệ thống.

Công việc thực hiện theo quý

- Thời gian thực hiện: ngày T6 của tuần cuối cùng trong tháng cuối quý (thời gian thực hiện tùy theo từng công việc và tuân thủ theo quy định cụ thể ghi trong phần thủ tục thực hiện của công việc).
- Người thực hiện: nhân viên chuyên trách quản lý hệ thống.

Công việc thực hiện hàng năm

- Thời gian thực hiện: tuần cuối của tháng 12 hàng năm.
- Người thực hiện: nhân viên chuyên trách quản lý hệ thống.

VI. Chức năng, nhiệm vụ của các đơn vị kỹ thuật tại Trung tâm

1. Phòng Kỹ thuật khai thác

- Quản lý, vận hành khai thác toàn bộ các thiết bị mạng và bảo mật tại Trung tâm (trừ một số thiết bị access do Chi nhánh Hồ chí minh quản lý) tại 04 site: Yên Hòa, Giáp Bát, Đà Nẵng và Hồ Chí Minh. Bao gồm các thiết bị router biên, các thiết bị firewall, coreswitch, router cp và các thiết bị access tại site Yên Hòa, Giáp Bát và Đà Nẵng.
  - Quản lý, khai báo, quy hoạch các kết nối tại các site Yên Hòa, Giáp Bát, Đà Nẵng và Hồ Chí Minh.
  - Cấp phát tài nguyên kết nối cho các hệ thống, dịch vụ.
  - Phối hợp xây dựng, đánh giá mức độ an toàn, phù hợp của các phương án kết nối cụ thể của từng hệ thống, dịch vụ trước và sau khi đưa vào hoạt động trong mạng tin học Trung tâm.
  - Quản lý định tuyến các hướng kết nối tới Mạng Tin học Trung tâm.
- Chủ trì phối hợp với các đơn vị trong Tổng Công ty và các đối tác các vấn đề liên quan, đảm bảo chất lượng hoạt động của Mạng Tin học Trung tâm.
- Lập phương án thực hiện các công việc nâng cấp, thay đổi tham số, các sự cố liên quan tới hệ thống mạng và bảo mật tại Trung tâm.

- Lập kế hoạch thực hiện định kỳ việc bảo trì bảo dưỡng Mạng Tin học Trung tâm.
- Lập kế hoạch định kỳ đánh giá chất lượng, độ khấu hao, đề xuất thay thế, nâng cấp phần mềm, phần cứng thiết bị mạng và bảo mật tại Trung tâm.
- Tham mưu đề xuất Lãnh đạo Trung tâm các vấn đề khác liên quan tới Mạng Tin học Trung tâm.

2. Chi nhánh Hồ Chí Minh

- Hỗ trợ, phối hợp với Phòng Kỹ thuật Khai thác, Phòng Phát triển Dịch vụ và các đối tác triển khai các công việc liên quan tới Mạng Tin học Trung tâm tại Chi nhánh Hồ Chí Minh.
- Phối hợp xử lý các sự cố xảy ra, các công việc nâng cấp, thay đổi tham số, sự cố liên quan tới hệ thống Mạng Tin học Trung tâm tại Chi nhánh Hồ Chí Minh.
- Quản lý hạ tầng bao gồm nguồn điện, điều hòa, phần cứng các thiết bị mạng và bảo mật Mạng Tin học Trung tâm tại Chi nhánh Hồ Chí Minh và các đường truyền, thiết bị kết nối tới Data Center CMC Hồ Chí Minh.
- Quản lý, vận hành, khai thác các thiết bị access bao gồm: các thiết bị mạng access tại Mạng Chi nhánh Hồ Chí Minh.
- Giám sát từ xa thông qua hệ thống Giám sát OMC tập trung các thiết bị mạng và bảo mật.
- Thực hiện các nhiệm vụ khác được Lãnh đạo Trung tâm giao.

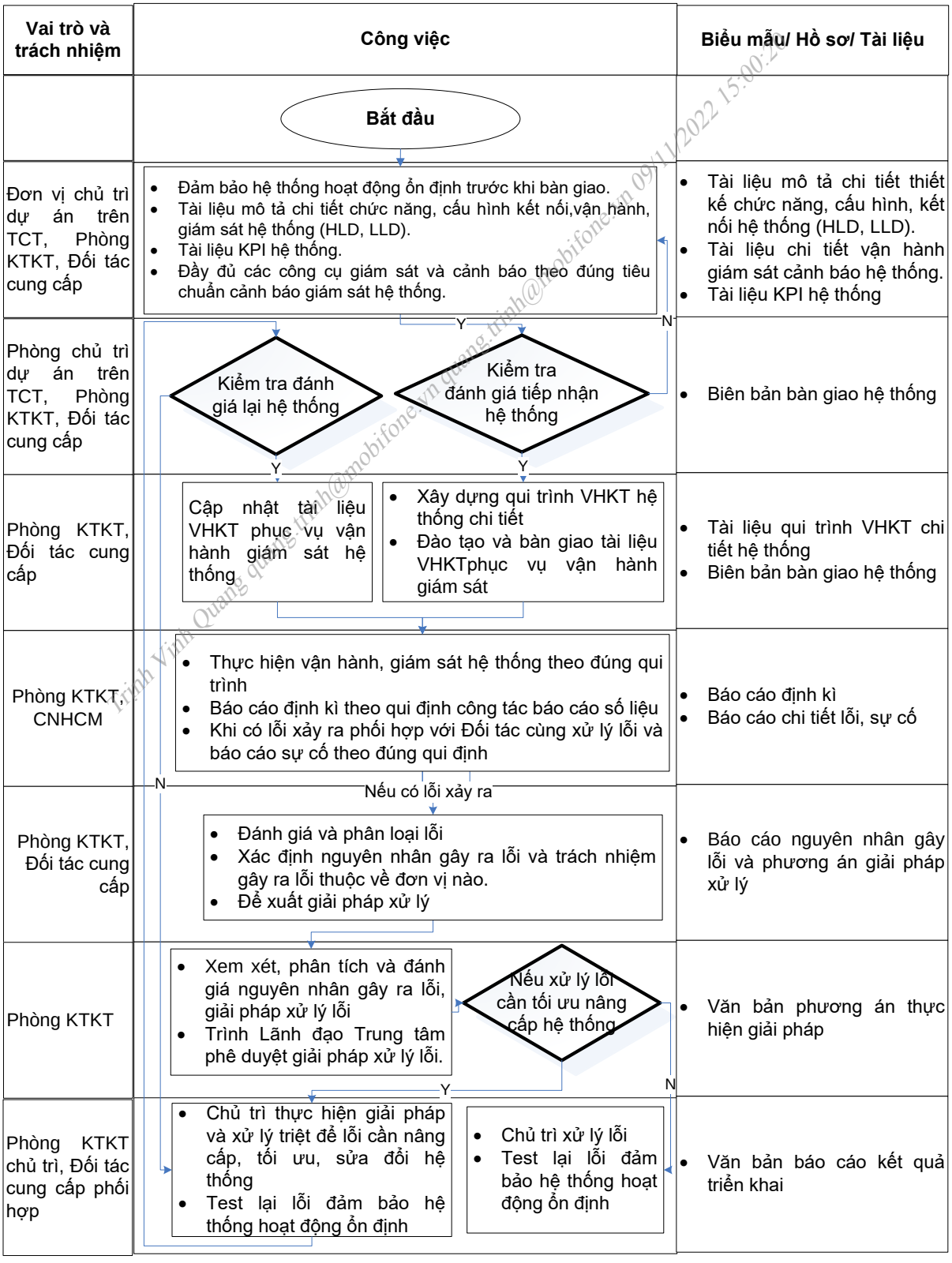
3. Phòng Phát triển Dịch vụ

- Phối hợp với Phòng Kỹ thuật Khai thác, Chi nhánh Hồ Chí Minh trong việc kết nối, khai báo các hệ thống dịch vụ giá trị gia tăng, các kết nối dịch vụ, kết nối phục vụ sản xuất kinh doanh và các vấn đề liên quan tới Mạng Tịn học Trung tâm.
- Thực hiện bàn giao các thiết bị mạng, firewall … của các hệ thống dịch vụ cho Phòng Kỹ thuật Khai thác khi đưa vào hoạt động.

B. NỘI DUNG QUY TRÌNH

I. Quy trình tiếp nhận và vận hành khai thác thiết bị mạng và bảo mật

1. Sơ đồ triển khai



2. Mô tả sơ đồ triển khai

2.1. Đơn vị chủ trì dự án Tổng Công ty bàn giao hệ thống

- Trước khi bàn giao hệ thống, Đơn vị chủ trì dự án trên Tổng Công ty chịu trách nhiệm:
  - Yêu cầu Đối tác đảm bảo hệ thống thiết bị mạng và bảo mật **phải đáp ứng các yêu cầu kỹ thuật nêu trong hợp đồng ký kết và hoạt động ổn định trong mạng Tin học của Trung tâm MDS.**
  - Yêu cầu Đối tác cung cấp đầy đủ các tài liệu mô tả chi tiết chức năng, cấu hình, kết nối, tài liệu vận hành khai thác.
  - Yêu cầu Đối tác cung cấp tài liệu KPI hệ thống.
  - Bàn giao bản sao Biên bản đào tạo có xác nhận các Trưởng đơn vị.
  - Yêu cầu Đối tác cung cấp tài liệu chi tiết về vận hành, khai thác, giám sát cảnh báo hệ thống.
  - Yêu cầu Đối tác cung cấp chi tiết thông tin liên lạc của các đầu mối hỗ trợ kỹ thuật để phối hợp với Phòng Kỹ thuật Khai thác xử lý trong quá trình vận hành giám sát và xử lý hệ thống.

2.2. Phòng Kỹ thuật Khai thác tiếp nhận hệ thống để quản lý vận hành khai thác

- Phòng Kỹ thuật Khai thác chịu trách nhiệm kiểm tra đánh giá và tiếp nhận hệ thống. Nếu hệ thống không đáp ứng đủ các yêu cầu thì kiến nghị Đơn vị chủ trì dự án trên Tổng Công ty có trách nhiệm yêu cầu Đối tác cung cấp bổ xung đầy đủ các yêu cầu.
- Lưu Biên bản bàn giao hệ thống từ Tổng Công ty để phục vụ công tác quản lý hệ thống.
- Sau khi tiếp nhận hệ thống, Phòng Kỹ thuật Khai thác chịu trách nhiệm xây dựng quy trình quản lý VHKT chi tiết hệ thống để ban hành áp dụng trong công tác điều hành quản lý khai thác hệ thống.

2.3. Phòng Kỹ thuật Khai thác vận hành giám sát theo đúng quy trình

- Phòng Kỹ thuật Khai thác thực hiện vận hành giám sát theo đúng quy trình VHKT chi tiết hệ thống. Phòng Kỹ thuật Khai thác có trách nhiệm giám sát theo dõi hệ thống và đảm bảo hệ thống hoạt động ổn định.
- Phòng Kỹ thuật Khai thác chịu trách nhiệm thực hiện báo cáo định kỳ cho ĐHKT cấp Trung tâm theo quy định công tác báo cáo số liệu các hệ thống thiết bị mạng

và bảo mật.

- Khi hệ thống xảy ra lỗi, Phòng Kỹ thuật Khai thác phối hợp với Đối tác cung cấp hệ thống cùng xử lý lỗi theo đúng quy định xử lý sự cố các hệ thống và báo cáo sự cố cho ĐHKT cấp Trung tâm.

2.4. Phòng Kỹ thuật Khai thác và Đối tác cung cấp xác định nguyên nhân gây ra lỗi và đề xuất giải pháp xử lý

- Phòng Kỹ thuật Khai thác phối hợp với Đối tác cung cấp thực hiện đánh giá và phân loại lỗi. Từ đó xác định nguyên nhân gây ra lỗi và trách nhiệm gây ra lỗi thuộc về đơn vị nào.
- Phòng Kỹ thuật Khai thác phối hợp với Đối tác cung cấp đề xuất giải pháp xử lý sự cố.

2.5. Phòng Kỹ thuật Khai thác phân tích đánh giá giải pháp và trình Lãnh đạo Trung tâm phê duyệt

- Phòng Kỹ thuật Khai thác trình Lãnh đạo trung tâm giải pháp khắc phục triệt để sự cố.

2.6. Phòng Kỹ thuật Khai thác phối hợp Đối tác thực hiện triển khai giải pháp

- Phòng Kỹ thuật Khai thác có trách nhiệm thực hiện giải pháp và xử lý sự cố triệt để theo văn bản Lãnh đạo Trung tâm đã phê duyệt.
- Phòng Kỹ thuật Khai thác chủ trì thực hiện giải pháp và xử lý triệt để các lỗi cần nâng cấp, tối ưu, sửa đổi phần mềm hoặc phần cứng hệ thống thiết bị mạng và bảo mật, đồng thời gửi các thông tin về việc thay đổi hệ thống cho Đơn vị chủ trì dự án trên Tổng Công ty. Nếu không cần nâng cấp, sửa đổi hệ thống thì Phòng Kỹ thuật Khai thác chủ trì thực hiện giải pháp và nghiệm thu lại hệ thống.
- Phòng Kỹ thuật Khai thác kiểm tra đánh giá lại hệ thống. Nếu hệ thống vẫn chưa được khắc phục triệt để sự cố thì Phòng Kỹ thuật Khai thác phải phối hợp Đối tác cung cấp thực hiện lại theo văn bản Lãnh đạo Trung tâm đã phê duyệt.
- Sau khi hoàn thành triển khai khắc phục, Phòng Kỹ thuật Khai thác làm văn bản báo cáo kết quả triển khai cho Lãnh đạo Trung tâm, thực hiện cập nhật lại tài liệu VHKT chi tiết hệ thống để đảm bảo cập nhật thông tin chính xác nhất về hệ thống.

3. Quy trình quản lý địa chỉ IP

3.1. Quy trình cấp phát địa chỉ IP

- Các căn cứ:
  + Đơn vị quản lý nhân sự đề nghị cấp phát bằng văn bản.
  + Văn bản thông báo nhân sự của phòng Tổng hợp.
  + Đề xuất bổ sung IP cho nhân viên cũ.
- Lưu đồ thực hiện:

Đơn vị	Công việc	Nội dung công việc
- Phòng/ban đề nghị cấp phát IP PC - Phòng Kỹ thuật khai thác - Phòng Tổng hợp	Bắt đầu OK	Đầu mối phòng yêu cầu cấp phát IP thực hiện gửi đề nghị cấp phát bằng văn bản bao gồm các thông tin: - Công văn giao nhân sự thử việc/chính thức/chuyên gia/chất lượng cao. - Văn bản đề xuất cấp thêm IP cho nhân sự cũ. - Phiếu yêu cầu cấp phát/thu hồi địa chỉ IP cho máy tính cá nhân.
- Phòng Kỹ thuật khai thác - Phòng Tổng hợp	Duyệt yêu cầu OK	Lãnh đạo phòng KTKT xét duyệt và phân công nhân sự thực hiện.
- Phòng đề nghị cấp phát IP PC - Phòng Kỹ thuật khai thác	Thực hiện cấp phát IP	Đầu mối cấp IP Phòng KTKT thực hiện cấp phát IP và gửi lại thông tin cho đầu mối phòng đề xuất trong vòng không quá 3 ngày sau khi nhận được văn bản, yêu cầu ký biên bản tiếp nhận sử dụng IP.
- Phòng Kỹ thuật khai thác	OK Kết thúc	Phòng KTKT thực hiện lưu hồ sơ quản lý IP và giám sát theo quy định.

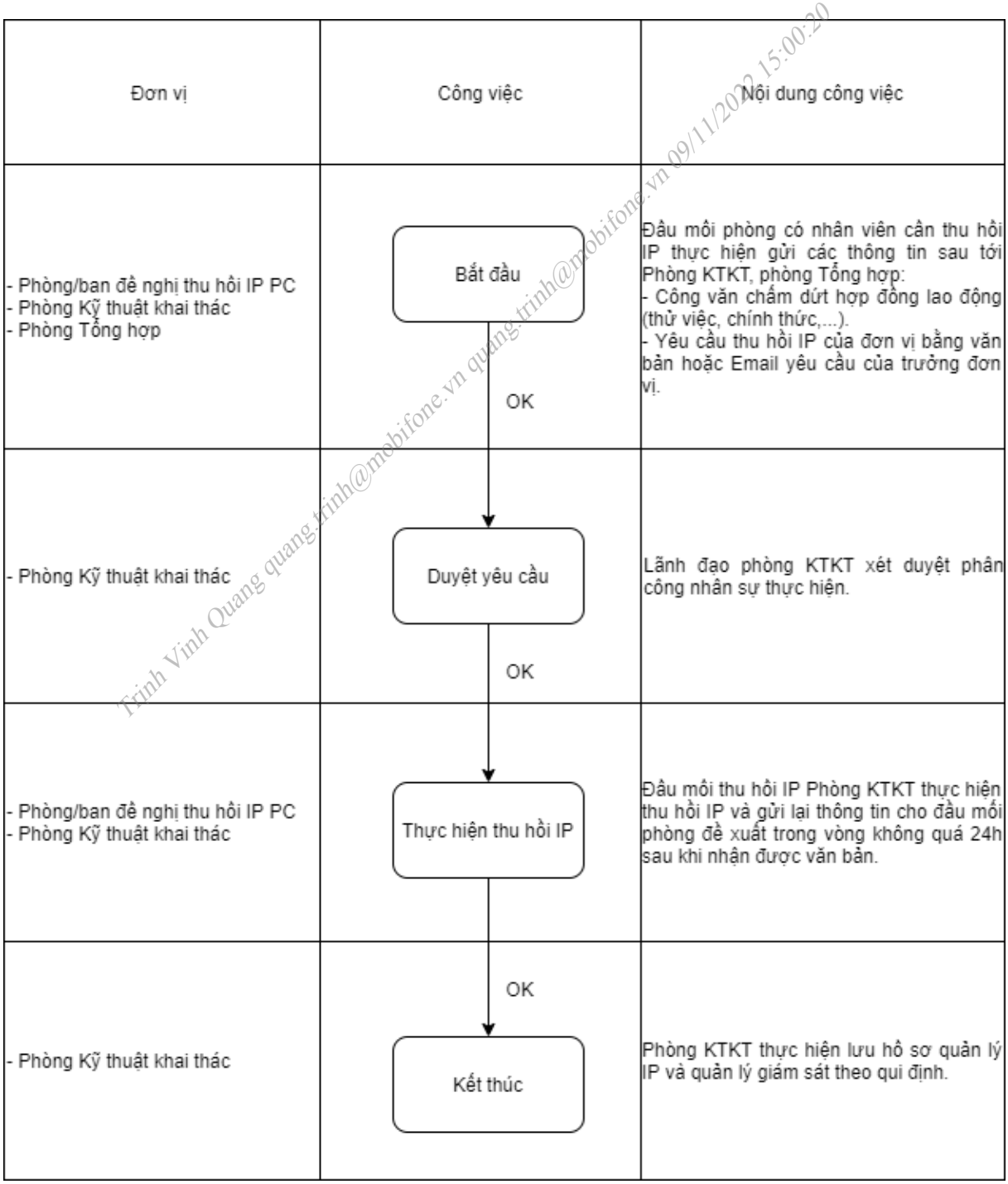
3.2. Quy trình thu hồi địa chỉ IP

- Các căn cứ:
  + Công văn thông báo chấm dứt hợp đồng lao động (chính thức, thử việc) của

phòng Tổng hợp.

+ Yêu cầu của đơn vị quản lý nhân sự bằng văn bản hoặc Email có xác nhận của lãnh đạo đơn vị.

- Lưu đồ thực hiện:



4. Quy trình khai báo kết nối trên các thiết bị Firewall

Đối với các hệ thống Fintech, Mobile Money, ứng tiền và các hệ thống thông tin cấp độ 3.

- Các căn cứ:
  + Công văn giao nhiệm vụ, công văn ngừng cung cấp dịch vụ có phê duyệt của lãnh đạo Trung tâm (nếu có)
  + Tờ trình yêu cầu đóng/mở kết nối Firewall có phê duyệt của lãnh đạo Trung tâm.
  + Email đề nghị có xác nhận của lãnh đạo đơn vị (trong trường hợp xử lý gấp và sẽ bổ sung các văn bản liên quan khác sau)

Đơn vị	Công việc	Nội dung công việc
- Phòng/ban đề xuất khai báo/hủy bỏ kết nối Firewall - Phòng Kỹ thuật khai thác	Bắt đầu OK	Đầu mối phòng đề xuất thực hiện gửi các thông tin sau tới đầu mối Phòng KTKT : • Công văn giao nhiệm vụ, công văn ngừng cung cấp dịch vụ có phê duyệt của Lãnh đạo Trung tâm (nếu có). • Tờ trình yêu cầu mở hoặc đóng kết nối Firewall có phê duyệt của lãnh đạo Trung tâm. • Email đề nghị có xác nhận của lãnh đạo đơn vị (trong trường hợp cần xử lý gấp).
- Phòng Kỹ thuật khai thác	Duyệt yêu cầu OK	Lãnh đạo phòng KTKT chuyển yêu cầu tới đầu mối khai báo kết nối Firewall của phòng KTKT.
- Phòng/ban đề xuất khai báo/hủy bỏ kết nối Firewall - Phòng Kỹ thuật khai thác	Thực hiện khai báo/hủy bỏ OK	1. Nhân sự phụ trách khai báo Firewall thực hiện khai báo, hủy bỏ kết nối Firewall trong vòng không quá 3 ngày làm việc. 2. P.KTKT thông báo tới đơn vị kết quả thực hiện để kiểm tra kết nối tới các hệ thống.
- Phòng Kỹ thuật khai thác	Kết thúc	1. Đơn vị xác nhận kết nối thành công. 2. Phòng KTKT thực hiện cập nhật hồ sơ khai báo/hủy bỏ kết nối Firewall để giám sát theo quy định.

Đối với các hệ thống dịch vụ còn lại.

- Các căn cứ:
  + Công văn phê duyệt khai báo của Lãnh đạo Trung tâm.
  + Công văn đề nghị của đơn vị chức năng có xác nhận của Lãnh đạo đơn vị.
  + Trong các trường hợp cần khai báo gấp, căn cứ vào email đề nghị khai báo, có xác nhận của lãnh đạo đơn vị. Sau đó đơn vị đề nghị khai báo bổ sung văn bản đề xuất làm căn cứ lưu hồ sơ thực hiện.
  + Trong trường hợp các kết nối đề nghị khai báo không thuộc phê duyệt của theo văn bản của Lãnh đạo Trung tâm, đơn vị chức năng cần thực hiện gửi văn bản và form đề nghị mở khai báo theo mẫu của phòng KTKT cung cấp.
- Lưu đồ thực hiện:

Đơn vị	Công việc	Nội dung công việc
- Phòng/ban đề xuất khai báo Firewall - Phòng KTKT	Bắt đầu OK	Đầu mối phòng đề xuất thực hiện gửi các thông tin sau tới Phòng KTKT: - Công văn giao nhiệm vụ có phê duyệt của Lãnh đạo trung tâm. - Công văn đề nghị của đơn vị chắc năng có xác nhận của Lãnh đạo đơn vị. - Email đề nghị có xác nhận của đơn vị chức năng. - Phiếu yêu cầu khai báo Firewall.
- Phòng Kỹ thuật khai thác	Duyệt yêu cầu OK	Lãnh đạo phòng KTKT chuyển yêu cầu tới đầu mối khai báo kết nối Firewall của phòng KTKT.
- Phòng/ban đề xuất khai báo kết nối Firewall - Phòng KTKT	Thực hiện khai báo	Nhân sự phụ trách khai báo Firewall thực hiện khai báo trong vòng không quá 3 ngày làm việc. P.KTKT thông báo tới đơn vị kết quả thực hiện để kiểm tra kết nối tới các hệ thống.
- Phòng KTKT	OK Kết thúc	Đơn vị xác nhận kết nối thành công, Phòng KTKT thực hiện cập hồ sơ khai báo để kết quả công việc và giám sát theo qui định.

II. Tài liệu quản lý vận hành khai thác các hệ thống mạng và bảo mật

Quy trình quản lý, vận hành khai thác các thiết bị mạng và bảo mật tại Trung tâm đảm bảo các tiêu chuẩn cơ bản sau:

- Đảm bảo an toàn thông tin các thiết bị mạng và bảo mật tại Trung tâm, các hệ thống, dịch vụ giá trị gia tăng.
- Thay thế, nâng cấp, chỉnh sửa cấu hình, mô hình kết nối cần có các phê duyệt của các cấp có thẩm quyền và thực hiện trong giờ thấp điểm.

- Đảm bảo các thiết bị luôn hoạt động ở chế độ dự phòng (active – active hoặc active – standby).

Quy trình quản lý, vận hành khai thác các thiết bị mạng và bảo mật tại Trung tâm bao gồm các quy trình vận hành các thiết bị sau:

- Quy trình quản lý, vận hành, khai thác thiết bị Firewall Checkpoint.
- Quy trình quản lý, vận hành, khai thác thiết bị Router Core.
- Quy trình quản lý, vận hành, khai thác thiết bị Switch Core.
- Quy trình quản lý, vận hành, khai thác thiết bị Router CP.
- Quy trình quản lý, vận hành, khai thác thiết bị switch access.

(chi tiết các quy trình tại phụ lục 01 gửi kèm)

III. Danh sách các thiết bị mạng và bảo mật tại Trung tâm.

1. Danh sách thiết bị mạng và bảo mật do Phòng Kỹ thuật Khai thác quản lý

STT	Thiết bị	Tên	Số lượng	Site	Vị trí	Ghi chú
1	ASRR9000	ASR9K-MDS-YHA	2	Yên Hòa	Tầng 6	
		ASR9K-MDS-GBT	2	Giáp Bát	Tầng 3	
		ASR9K-MDS-ĐNG	2	An Đồn	Tầng 4	
		ASR9K-MDS-HCM	2	MM18	Tầng 1	
2	Firewall	MDS-FW15400-YHA	2	Yên Hòa	Tầng 6	
		MDS-FW5070-GBT	2	Yên Hòa	Tầng 6	
		MDS-FW5070-ĐNG	2	Giáp Bát	Tầng 5	
		MDS-FW5070-HCM	2	An Đồn	Tầng 4	
		MDS-FW9070-HCM	2	MM18	Tầng 1	
		MDS-FG-1101-YHA	2	Yên	Tầng 6	

				Hòa		
		MDS-FG-1101-HCM	2	MM18	Tầng 1	
3	Router truyền dẫn	Router_CP_7606_YHA	1	Yên Hòa	Tầng 4	
		Router_CP_7606_HCM	1	MM18	Tầng 1	
		Router_CP_7613_YHA	2	Yên Hòa	Tầng 4	
		Router_CP_7613_HCM	2	MM18	Tầng 1	
4	Router hệ thống CRBT	Router_CRBT	2	Giáp Bát	Tầng 3	
5	CoreSwitch 6509	CS6509_YHA	2	Yên Hòa	Tầng 6	
		CS6509_GBT	2	Giáp Bát	Tầng 5	
		CS6509_ĐNG	2	An Đồn	Tầng 4	
		CS6509_HCM	2	MM18	Tầng 1	
6	Switch Access	SW_Acc_YHA	21	Yên Hòa	Tầng 4, 6	
		SW_Acc_GBT	4	Giáp Bát	Tầng 2, 3, 5	
		SW_Acc_ĐNG	2	An Đồn	Tầng 2	
		SW_Acc_HCM	2	MM18	Tầng 1	

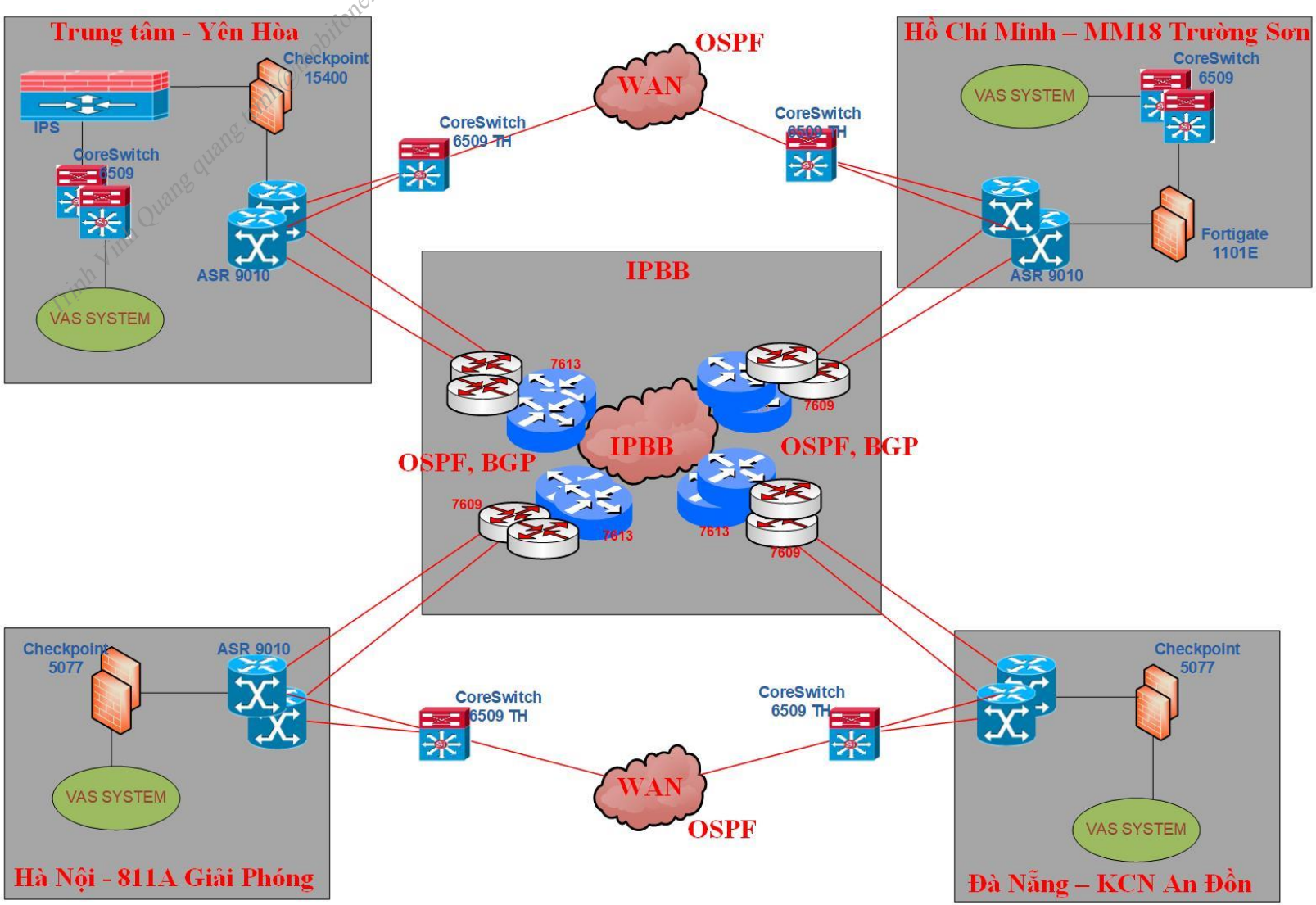
2. Danh sách thiết bị mạng và bảo mật do Chi nhánh Hồ Chí Minh phối hợp quản lý

STT	Thiết bị	Tên	Số lượng	Site	Vị trí	Ghi chú
1	ASR9000	ASR9K-MDS-HCM	2	MM18	Tầng 1	Quản lý phần

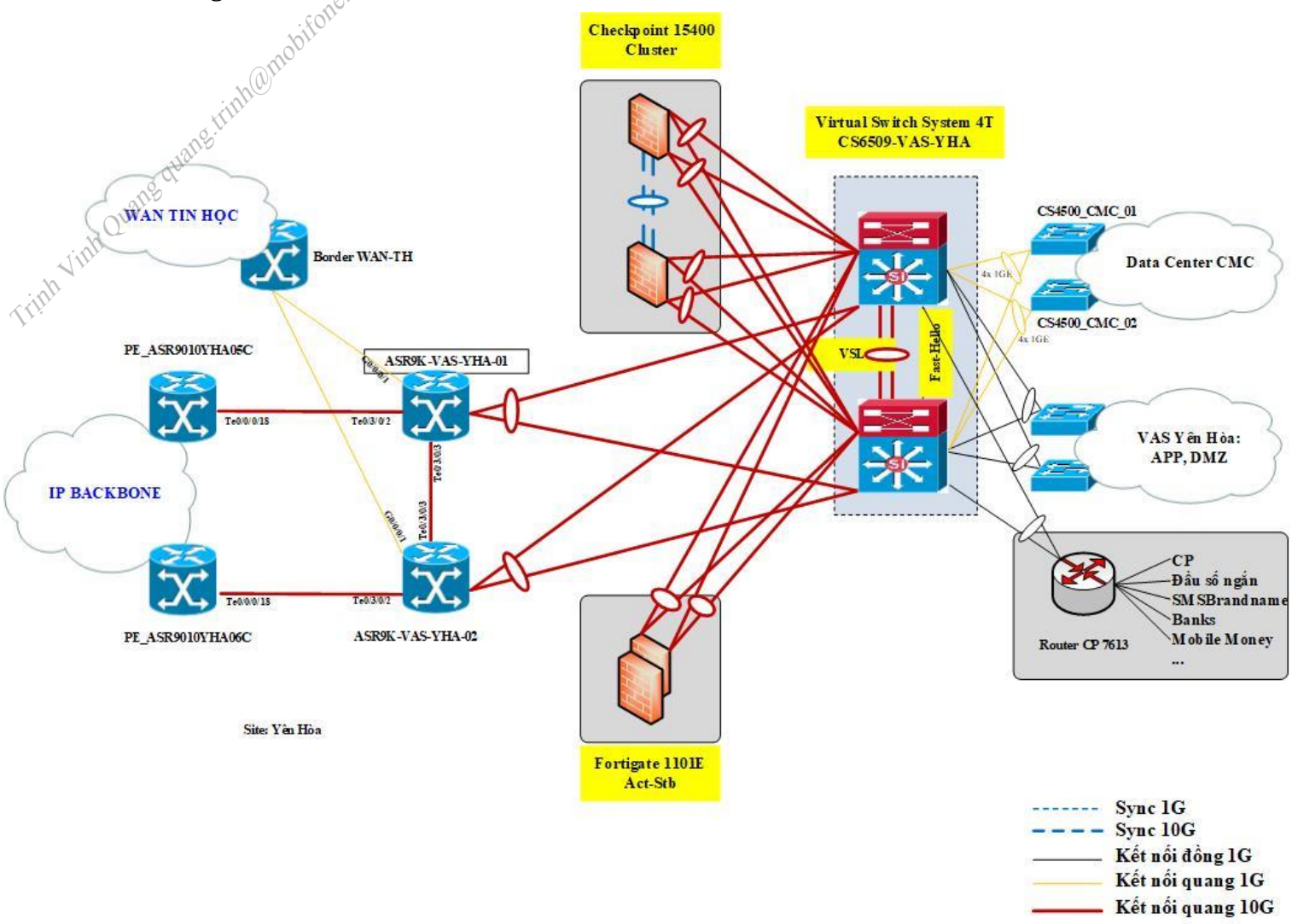
2	Firewall	MDS-FW5070-HCM	2	MM18	Tầng 4	cứng, hạ tầng nguồn điện. Hỗ trợ phòng Kỹ thuật khai thác và đối tác vào ra phòng máy.
		MDS-FW9070-HCM	2	MM18	Tầng 1	
		MDS-FG-1101-HCM	2	MM18	Tầng 1	
3	Router truyền dẫn	Router_CP7613_HCM	2	MM18	Tầng 1	
		Router_CP7606_HCM	1	MM18	Tầng 1	
4	Coreswitch	CS6509_HCM	2	MM18	Tầng 1	
5	Switch access	Sw_Acc_HCM	2	MM18	Tầng 1	

IV. Sơ đồ kết nối Mạng Tin học Trung tâm

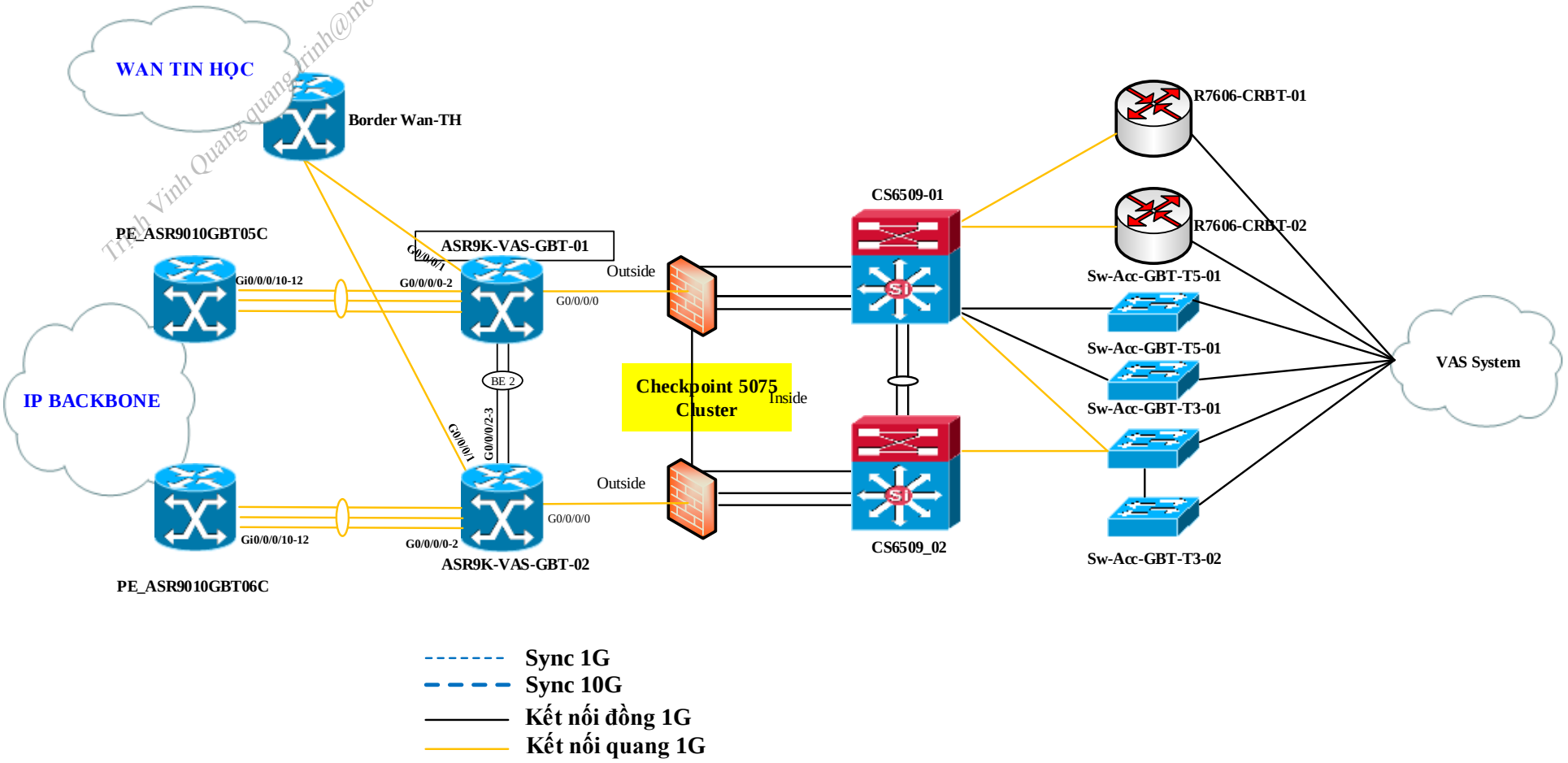
– Sơ đồ kết nối các site:



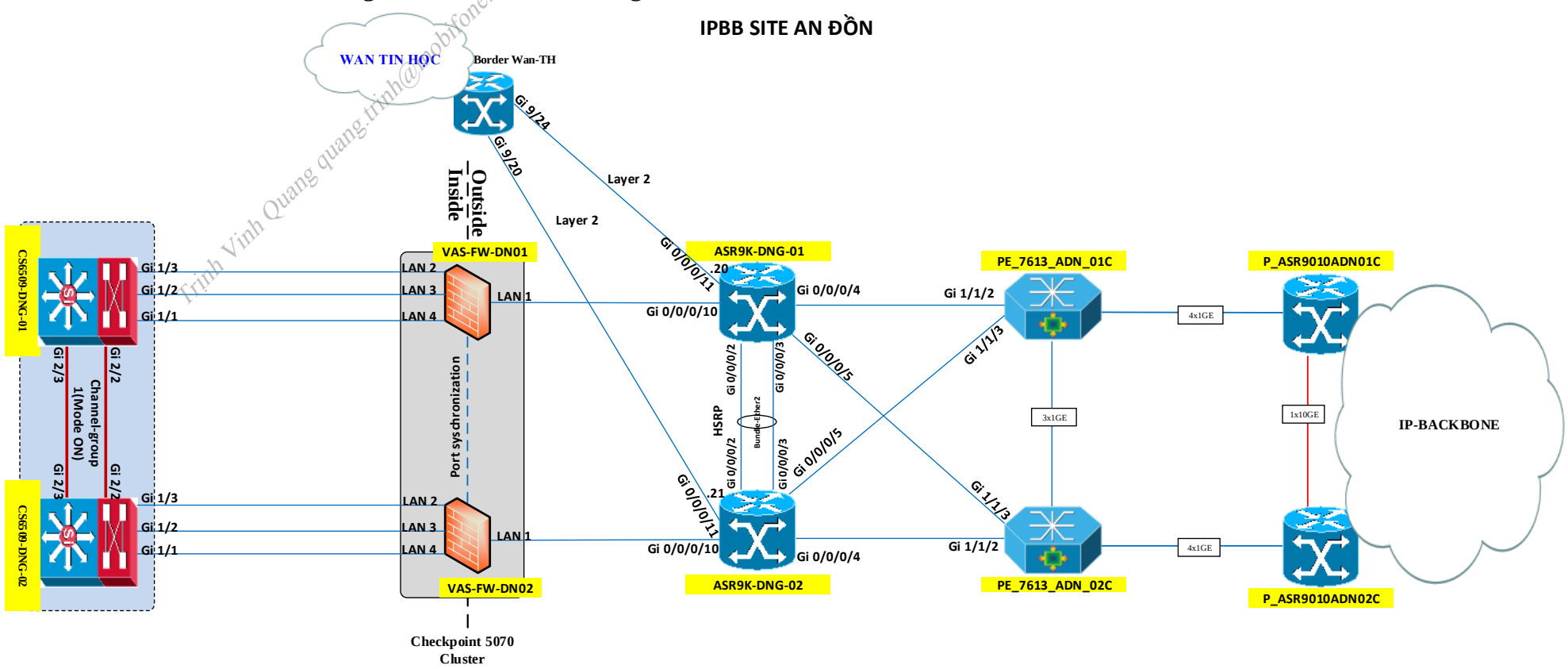
– Sơ đồ kết nối thiết bị mạng và bảo mật tại Yên Hòa.



– Sơ đồ kết nối thiết bị mạng và bảo mật tại Giáp Bát.

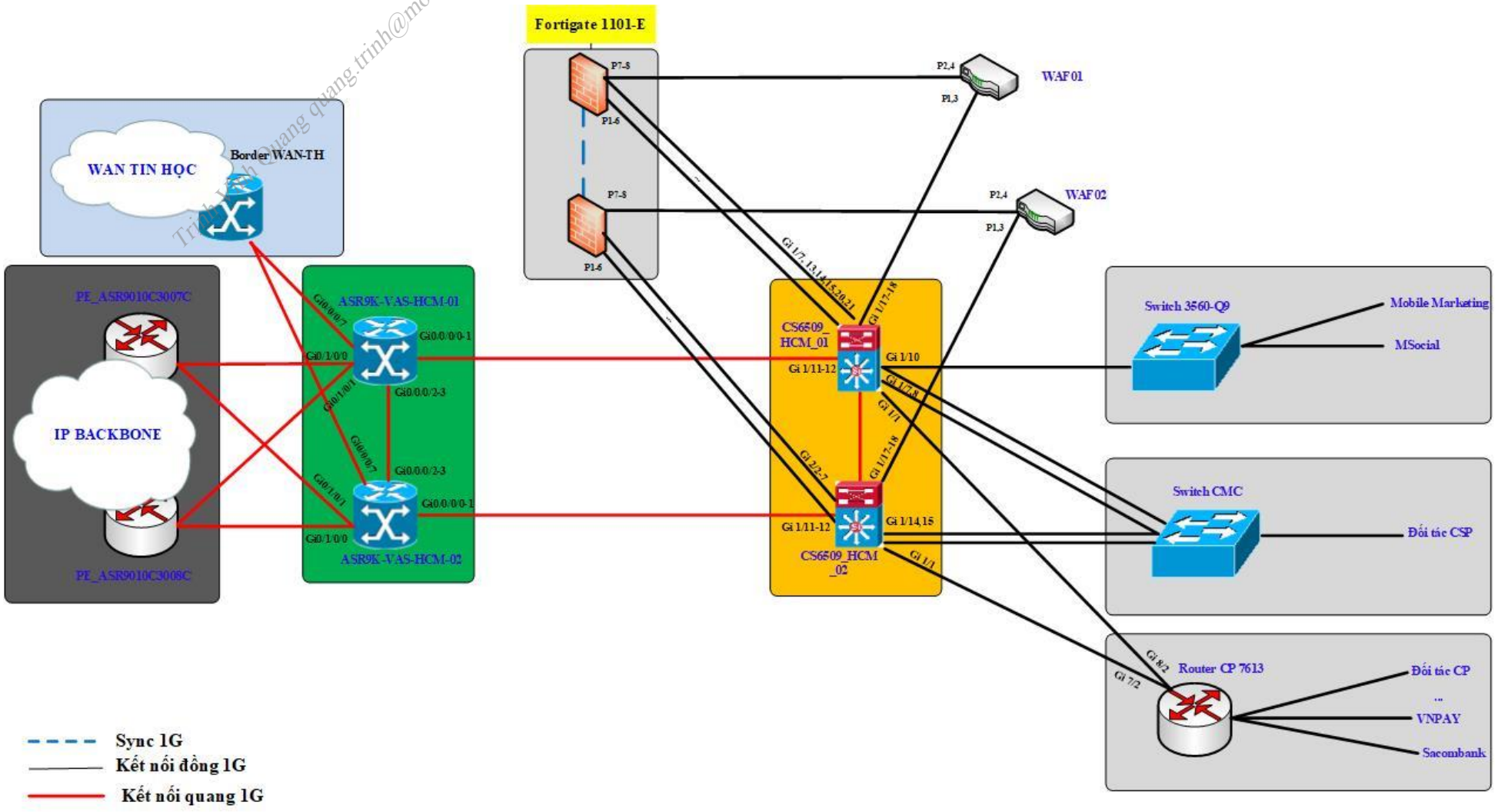


– Sơ đồ kết nối thiết bị mạng và bảo mật tại Đà Nẵng.

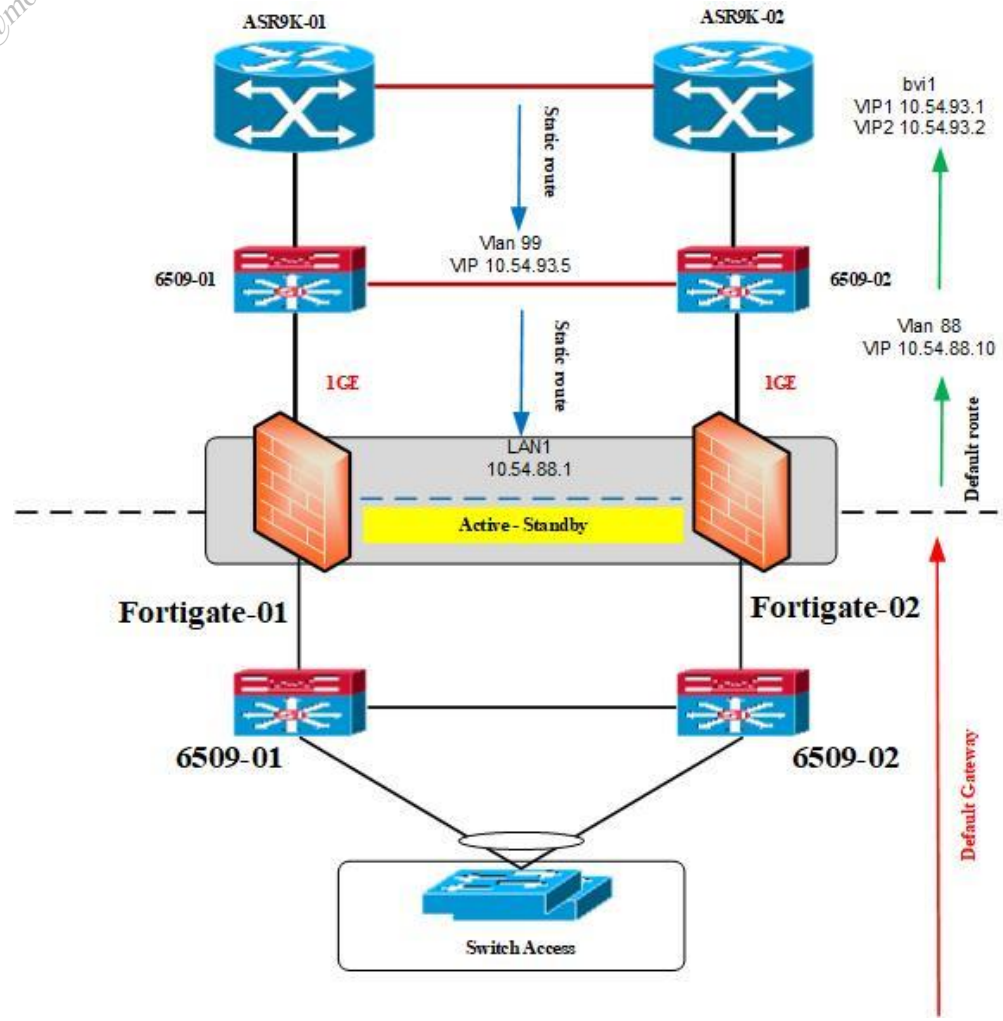


– Sơ đồ kết nối thiết bị mạng và bảo mật tại Hồ Chí Minh.

- Sơ đồ vật lý



- Sơ đồ logic



V. Nội dung các quy định, tiêu chuẩn quản lý vận hành khai thác

1. Quy định vận hành khai thác hệ thống thiết bị mạng và bảo mật

Tuân thủ theo Quy trình quản lý vận hành khai thác các hệ thống thiết bị mạng và bảo mật đã được Tổng Giám đốc Tổng Công ty hoặc Giám đốc Trung tâm phê duyệt.

2. Tiêu chuẩn giám sát cảnh báo hệ thống thiết bị mạng và bảo mật

- Tất cả các phân hệ của hệ thống thiết bị mạng và bảo mật phải có đầy đủ giám sát cảnh báo qua SMS và email khi phân hệ gặp lỗi hoặc ngừng hoạt động.
- Tất cả các thiết bị mạng và bảo mật phải được tích hợp và thực hiện giám sát trên hệ thống giám sát tập trung OMC.
- Tiêu chuẩn giám sát thông qua giao thức SNMP.

3. Giám sát cảnh báo các kết nối tới các hệ thống core của Mobifone

- Tất các các kết nối quan trọng tới các hệ thống core của Mobifone đều phải có giám sát cảnh báo qua SMS và Mail khi bị mất kết nối hoặc bị lỗi. Ví dụ:
  - Hướng kết nối tới mạng IPBB.
  - Hướng kết nối tới mạng Wan Tin học.
  - Hướng kết nối tới các hệ thống core: Charging Proxy, SMSC, SMPP, IN ...
- Cảnh báo giám sát thông qua hệ thống giám sát tập trung OMC.

4. Giám sát cảnh báo phần cứng các hệ thống thiết bị mạng và bảo mật

- Cảnh báo về phần cứng của hệ thống server triển khai các ứng dụng phần mềm của hệ thống thiết bị mạng và bảo mật bao gồm các cảnh báo sau:
  - Cảnh báo tình trạng sử dụng CPU, RAM. Khi CPU, RAM cao tải (lớn hơn 50%) phải có cảnh báo thông tin sử dụng CPU, RAM qua SMS hoặc Mail.
  - Cảnh báo dung lượng ổ cứng của các Server khi dung lượng ổ cứng gần đầy (lớn hơn 80 % dung lượng).
- Cảnh báo giám sát thông qua hệ thống giám sát tập trung OMC.

5. Giám sát cảnh báo phầm mềm của các hệ thống thiết bị mạng và bảo mật

- Phân quyền các account vào hệ thống để vận hành và giám sát hệ thống cho ĐHKT cấp Chi nhánh và đầu mối thiết bị mạng và bảo mật.
- Trường hợp các đơn vị có nhu cầu giám sát và nhận cảnh báo liên hệ với Phòng KTKT để tạo tài khoản và phạm vi giám sát (các yêu cầu gửi qua văn bản).

6. Quy định cấp phát các tài khoản truy nhập quản lý giám sát hệ thống thiết bị mạng và bảo mật, tài khoản VPN.

- Phòng Kỹ thuật Khai thác điều hành chịu trách nhiệm quản lý tài khoản và phân quyền, cấp phát tài khoản đúng chức năng và quyền cho các đơn vị khác thuộc Trung tâm các tài khoản có quyền quản lý giám sát hệ thống thiết bị mạng và bảo mật do Phòng Kỹ thuật Khai thác điều hành quản lý vận hành giám sát hệ thống.
- Mật khẩu của tài khoản phải theo đúng quy định: độ dài tối thiểu 8 ký tự bao gồm cả ký tự chữ, ký tự số và ký tự đặc biệt.
- Các đơn vị được cấp phát tài khoản sử dụng tài khoản đúng mục đích. Các đơn vị nhận được tài khoản phải có trách nhiệm bảo mật tài khoản được cấp phát và hàng tháng thay đổi mật khẩu theo quy định.
- ĐHKT cấp Trung tâm chịu trách nhiệm quản lý các tài khoản VPN cấp phát cho các đơn vị truy cập vào hệ thống để vận hành giám sát.

7. Các yêu cầu kỹ thuật của hệ thống thiết bị mạng và bảo mật:

7.1. Đảm bảo tính sẵn sàng cao (High Availability):

- Phải có mô hình dự phòng 1+1.
- Hệ thống có khả năng hoạt động liên tục 24x7.
- Dung lượng ổ cứng của hệ thống đáp ứng khả năng lưu trữ tương ứng với lưu lượng của hệ thống và số user hệ thống cam kết phục vụ.

7.2. Bảo mật:

- Hệ thống thiết bị mạng và bảo mật phải có cơ chế Backup và Recovery.
- Các truy cập từ xa đến hệ thống để hỗ trợ kỹ thuật phải được thực hiện qua VPN (có Token key để xác thực)
- Không được phép cài các phần mềm không hợp pháp, các phần mềm backdoor trên hệ thống nhằm tránh các nguy cơ mất an toàn bảo mật.
- Chỉ mở các port TCP/UDP liên quan cần thiết để chạy dịch vụ theo các văn bản phê duyệt, các port không cần thiết phải được chặn lại.
- Hệ thống phải có cơ chế ghi log các tác động lên hệ thống bao gồm:
    - File log lưu trữ ghi lại tác động của người vận hành khai thác, quản trị hệ thống như là : read, write, modify, delete.

- Hệ thống phải bật mặc định các tính năng bảo mật như anti spoofing, tính năng firewall, tính năng URL, App Control …

7.3. Tài liệu kiểm tra chất lượng hệ thống:

- Có kịch bản kiểm thử đầy đủ các tính năng hệ thống.
- Xây dựng kịch bản và cập nhật hàng năm cho phù hợp với thực tế hoạt động.

7.4. Quy định báo cáo và xử lý sự cố:

- Cung cấp các bước xử lý sự cố khi xảy ra sự cố trên hệ thống.

7.5. Quy định lưu trữ nhật ký thiết bị mạng và bảo mật

- Dữ liệu nhật ký thiết bị được lưu trực tuyến tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm.
- Chức năng ghi nhật ký và thông tin nhật ký được bảo vệ chống giả mạo, thay đổi và truy cập trái phép; bảo đảm người quản trị hệ thống và người sử dụng không thể xóa hay sửa đổi nhật ký hệ thống ghi lại hoạt động của chính họ.

8. Quy định kiểm tra đảm bảo chất lượng các hệ thống thiết bị mạng và bảo mật

8.1. Kiểm tra định kỳ

- Cơ sở hạ tầng:
  - Thời gian kiểm tra: 1 lần/quý.
  - Đơn vị thực hiện: Phòng Kỹ thuật Khai thác chủ trì, Phòng Phát triển Dịch vụ, Chi nhánh Hồ Chí Minh phối hợp.
  - Các nội dung kiểm tra: Phòng máy, cơ sở hạ tầng lắp đặt thiết bị đã đưa vào khai thác phục vụ khách hàng; cập nhật hồ sơ quản lý hệ thống thiết bị mạng và bảo mật. Khai báo, quản lý kết nối, hướng kết nối theo văn bản phê duyệt, văn bản quy định.
- Chất lượng hoạt động hệ thống:
  - Thời gian kiểm tra: 1 lần/tháng/hệ thống.
  - Đơn vị thực hiện: Phòng Kỹ thuật Khai thác chủ trì, Phòng Phát triển Dịch vụ, Chi nhánh Hồ Chí Minh phối hợp.
  - Các nội dung kiểm tra: đánh giá chất lượng các hệ thống thiết bị mạng và bảo mật cụ thể như bảng dưới. Các tiêu phí đánh giá chất lượng được xây dựng và cập nhật hàng năm, phù hợp với điều kiện hoạt động và điều kiện công

nghệ tại thời điểm thực hiện.

- Yêu cầu kiểm tra vật lý và cấu hình phần cứng thiết bị:
    - Kiểm tra nguồn điện vào thiết bị. Xác định nguồn điện đầu vào của thiết bị là bao nhiêu, có dự phòng nguồn không, điện áp hoạt động là bao nhiêu.
    - Kiểm tra cấu hình phần cứng. Đánh giá cấu hình phần cứng thiết bị còn hoạt động tốt, hỏng, hay đã hỏng một phần…, xác định dòng thiết bị còn được hỗ trợ từ hãng, support từ hãng hay không.
    - Kiểm tra phiên bản phần mềm IOS sử dụng trong các thiết bị. So sánh phiên bản IOS của hãng công bố, xác định tính phù hợp với yêu cầu mạng tin học Trung tâm MDS, khả năng bảo mật của thiết bị để đưa ra khuyến nghị về kế hoạch nâng cấp. Hỗ trợ thực hiện theo yêu cầu của Trung tâm MDS.
    - Kiểm tra phân tích Log file. Phân tích log file các thiết bị router, switch, firewall, từ đó dự báo, đưa ra các nguy cơ tiềm ẩn, dự đoán các lỗi có thể xảy ra.
    - Kiểm tra hoạt động của các linecard, các card điều khiển SUP, các card fan … Xác định các quạt có nguy cơ hỏng, hoạt động chập chờn, tìm kiếm thiết bị phù hợp và đề xuất phương án thay thế.
- Yêu cầu kiểm tra hoạt động của thiết bị, module mạng.
    - Kiểm tra hoạt động của thiết bị: Kiểm tra trạng thái CPU, Memory …
    - Kiểm tra hoạt động của hệ thống quạt: tình trạng hoạt động: tốt/ hỏng, thống số quạt …
    - Kiểm tra hoạt động của card điều khiển và đánh giá tính dự phòng của các card điều khiển trên các thiết bị tương ứng.
- Yêu cầu kiểm tra định tuyến
    - Kiểm tra giao thức định tuyến (nếu có). Thực hiện đồng bộ bảng định tuyến giữa các thiết bị, khả năng hội tụ giữa các thiết bị.
    - Kiểm tra bảng định tuyến (nếu có). Thực hiện đồng bộ bảng định tuyến giữa các site tại Mạng Tin học Trung tâm.

- Yêu cầu kiểm tra trạng thái kết nối.
    - Kiểm tra kết nối trực tiếp qua địa chỉ MAC.
    - Kiểm tra các thiết bị liền kề, xác định các giao diện uplink, downlink, update toàn bộ hệ thống mạng.
    - Kiểm tra các kết nối đang hoạt động và xác định các kết nối up, các kết nối down. Với các kết nối down thực hiện xác định kết nối còn hoạt động hay không và thực hiện up kết nối (nếu cần thiết)
    - Kiểm tra thông tin VTP, xác định khả năng hội tụ bảng vlan table, xác định thiết bị đóng vai trò server, thiết bị đóng vai trò client, trong trường hợp lỗi xảy ra, lập phương án cấu hình lại VTP.
    - Kiểm tra thông tin VLAN. Lập bảng Vlan toàn bộ dải mạng tại mạng tin học Trung tâm, thông tin bảng: STT, Vlan ID, Network/ Subnet, Descrtiption.
    - Kiểm tra thông tin các cổng trunking. Lập bảng vlan trunking giữa các thiết bị mạng tại các site Trung tâm.
- Yêu cầu kiểm tra hoạt động của thiết bị: khả năng bộ nhớ và bộ vi xử lý đáp ứng tài nguyên Ram.
- Yêu cầu thực hiện sao lưu cấu hình định kỳ và hỗ trợ nâng cấp phiên bản hệ điều hành mới hoặc theo cảnh báo của hãng (nếu phiên bản os hiện tại xảy ra các lỗi cần nâng cấp).
- Kiểm tra môi trường đặt thiết bị và làm vệ sinh công nghiệp.

- Kiểm tra đột xuất
    - Phòng Kỹ thuật Khai thác kiểm tra đột xuất.

VI. Điều khoản thi hành

- Các đơn vị được giao nhiệm vụ quản lý vận hành khai thác thiết bị mạng và bảo mật tại Trung tâm, thực hiện theo các nội dung quy định tại quy trình này.
- Phòng Kỹ thuật Khai thác có nhiệm vụ theo dõi, đôn đốc, đào tạo các cán bộ nhân viên thực hiện đúng quy trình.
- Trong quá trình thực hiện, nếu phát hiện nội dung quy định trong quy trình không phù hợp với điều kiện vận hành khai thác thực tế, các đơn vị làm văn bản báo cáo

Giám đốc Trung tâm xem xét sửa đổi.

VII. Lưu trữ hồ sơ

- Số liệu, báo cáo kiểm tra chi tiết có thể lưu trữ dưới dạng mềm (file, cơ sở dữ liệu máy tính), hoặc dưới dạng cứng (hồ sơ, tài liệu).
- Báo cáo đánh giá, tổng hợp kết quả kiểm tra lưu dưới dạng cứng (hồ sơ, tài liệu).

STT	Tên hồ sơ	Nơi lưu	Thời gian lưu
1	Kết quả kiểm tra phòng máy, cơ sở hạ tầng lắp đặt thiết bị đã đưa vào khai thác phục vụ khách hàng	– Phòng Kỹ thuật Khai thác – Phòng Tổng hợp	02 năm
2	Kết quả đánh giá chất lượng QoS các dịch vụ THIẾT BỊ MẠNG VÀ BẢO MẬT		
3	Hồ sơ quản lý cấu hình hệ thống các dịch vụ THIẾT BỊ MẠNG VÀ BẢO MẬT		

VIII. Phụ lục

1. Phụ lục 01: Các quy trình vận hành khai thác hệ thống thiết bị mạng và bảo mật.
2. Phụ lục 02: Danh sách thiết bị mạng bảo mật do phòng Kỹ thuật Khai thác quản lý.
3. Phụ lục 03: Biểu mẫu đánh giá hệ thống.
4. Phụ lục 04: Các biểu mẫu đăng ký.

VII. Danh sách đầu mối phối hợp

STT	Họ và tên	Đơn vị	Chức vụ	Địa chỉ Email	Số điện thoại
1	Nguyễn Việt Hùng	Phòng KTKT	Trưởng phòng KTKT	hung.nguyen@mobifone.vn	0904223388
2	Bùi An Lộc	Phòng KTKT	Phó phòng KTKT	loc.buian@mobifone.vn	0904383300
3	Hoàng Bảo Trung	Phòng KTKT	Chuyên viên phòng KTKT	trung.hoang@mobifone.vn	0901668666
4	Nguyễn Hữu Đức	Phòng KTKT	Chuyên viên phòng KTKT	duc.nguyenhuu@mobifone.vn	0777379997
5	Phạm Hồng Phúc	CNHCM	Phó giám đốc CN	phuc.pham@mobifone.vn	0903997878
6	Võ Thị Thùy Hạnh	CNHCM	Tổ trưởng tổ hỗ trợ kỹ thuật	hanh.vo@mobifone.vn	0909238855
7	Trần Minh Phúc	CNHCM	Tổ hỗ trợ kỹ thuật	phuc.minh@mobifone.vn	0909432109

PHỤ LỤC 01. TÀI LIỆU QUẢN LÝ VẬN HÀNH KHAI THÁC CÁC HỆ THỐNG MẠNG VÀ BẢO MẬT

- Tài liệu vận hành khai thác thiết bị Firewall Checkpoint.
- Tài liệu vận hành khai thác thiết bị Router Cisco ASR9000.
- Tài liệu vận hành khai thác thiết bị CoreSwitch 6509.
- Tài liệu vận hành khai thác thiết bị Switch Aceess.

I. Tài liệu vận hành khai thác thiết bị Firewall Checkpoint

1. Backup cấu hình:

- **Trên Gateway Security:** Thực hiện các câu lệnh dưới và lưu thông tin.

```
VAS-FW-YH-01> show configuration
#
# Configuration of VAS-FW-YH-01
# Language version: 12.3v1
#
# Exported by admin on Fri Aug 30 15:46:13 2019
#
set lcd screensaver mode model
set lcd screensaver timeout 30
set snmp mode default
set snmp agent on
set snmp agent-version any
set snmp community public read-only
set snmp community public read-write
…
```

```
[Expert@VAS-FW-YH-02:0]# cpinfo
This is Check Point CPinfo Build 914000173 for GAIA
Checking for updates...
        Updating...
Verifying CK...
```

- **Trên CMA (Smart Dashboard)**

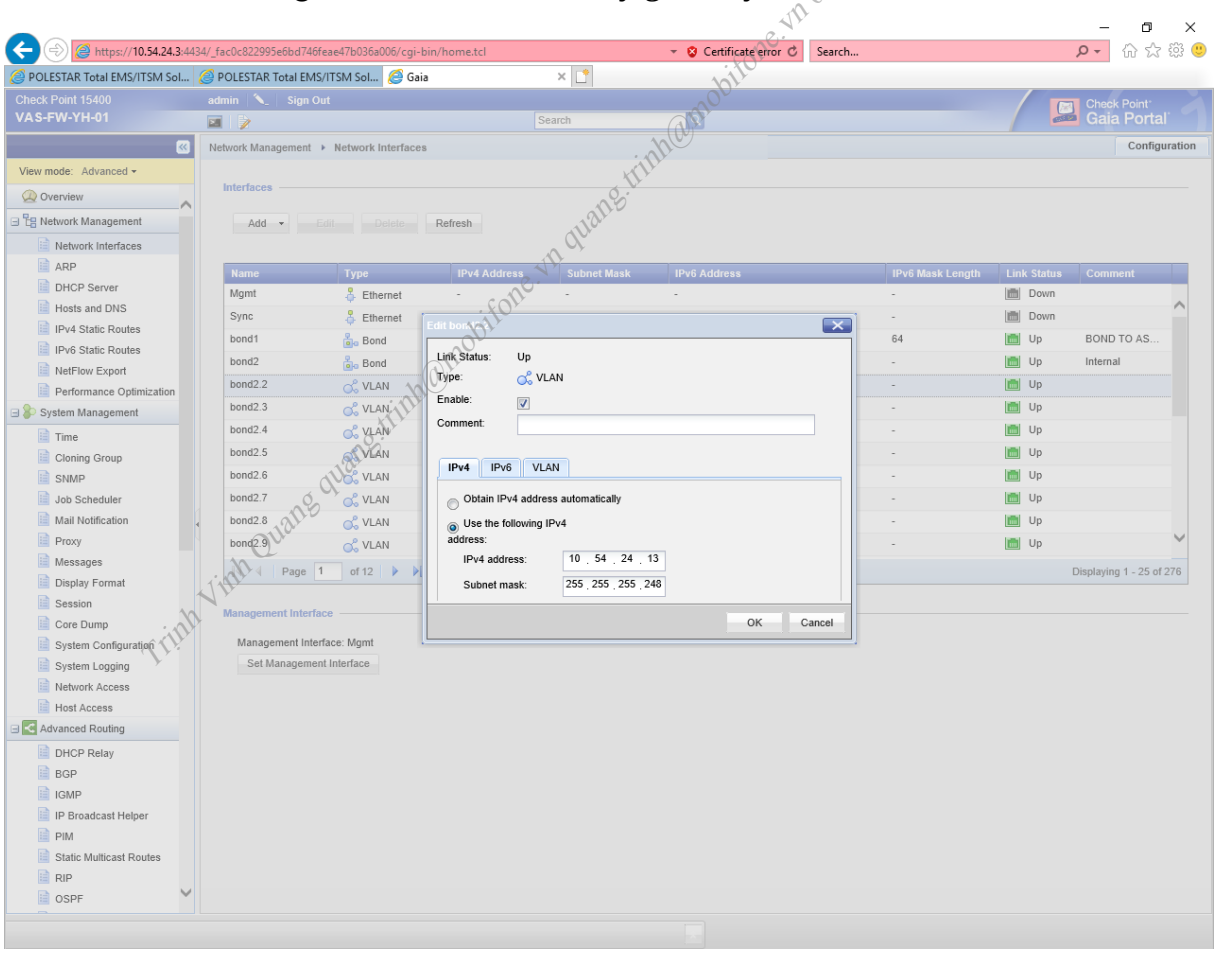
CMA thực hiện lưu giữ tập trung các policy, các đối tượng network, host, VPN … và được lưu trữ tập trung trên thiết bị Provider – 1 của Tổng Công ty. CMA dùng để điều kiển các cặp security gateway.

2. Khai báo các lớp mạng

- Đăng nhập giao diện quản trị trên security gateway. Thực hiện khai báo IP gateway cho các lớp mạng.

  Click *Network Interface* → *Add* → *Vlan.*

  Thực hiện tương tự trên thiết bị security gateway còn lại.



- Đăng nhập giao diện quản trị Smart Dashboard. Thực hiện khai báo IP Cluster cho lớp mạng:

  Trên giao diện *Smart Dashboard* → *Click Checkpoint* → *Chọn Cluster cần khai báo lớp mạng mới* →

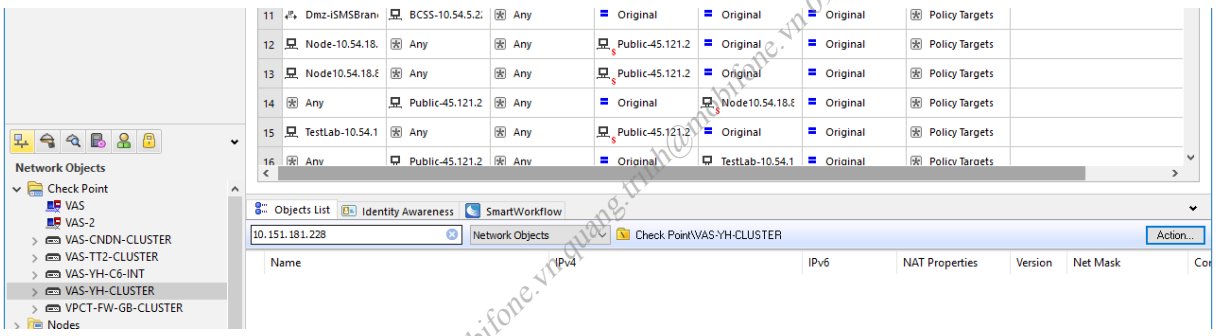
  Trên giao diện *Gateway Cluster Properties* → *Topology* → *Details*

Trên giao diện *Edit Topology → Get → Get All Topology → chọn các lớp mạng vừa khai báo trên các Security Gateway và khai báo địa chỉ IP Cluster cho lớp mạng đó.*

Các host khi được cấp phát IP trên lớp mạng đó sẽ nhận IP Cluster làm gateway.

3. Khai báo các đối tượng mạng

- Đăng nhập giao diện Smart Dashboard → Click Action → New → Chọn các đối tượng mạng cần khai báo (Network, Checkpoint, Host, Range …).

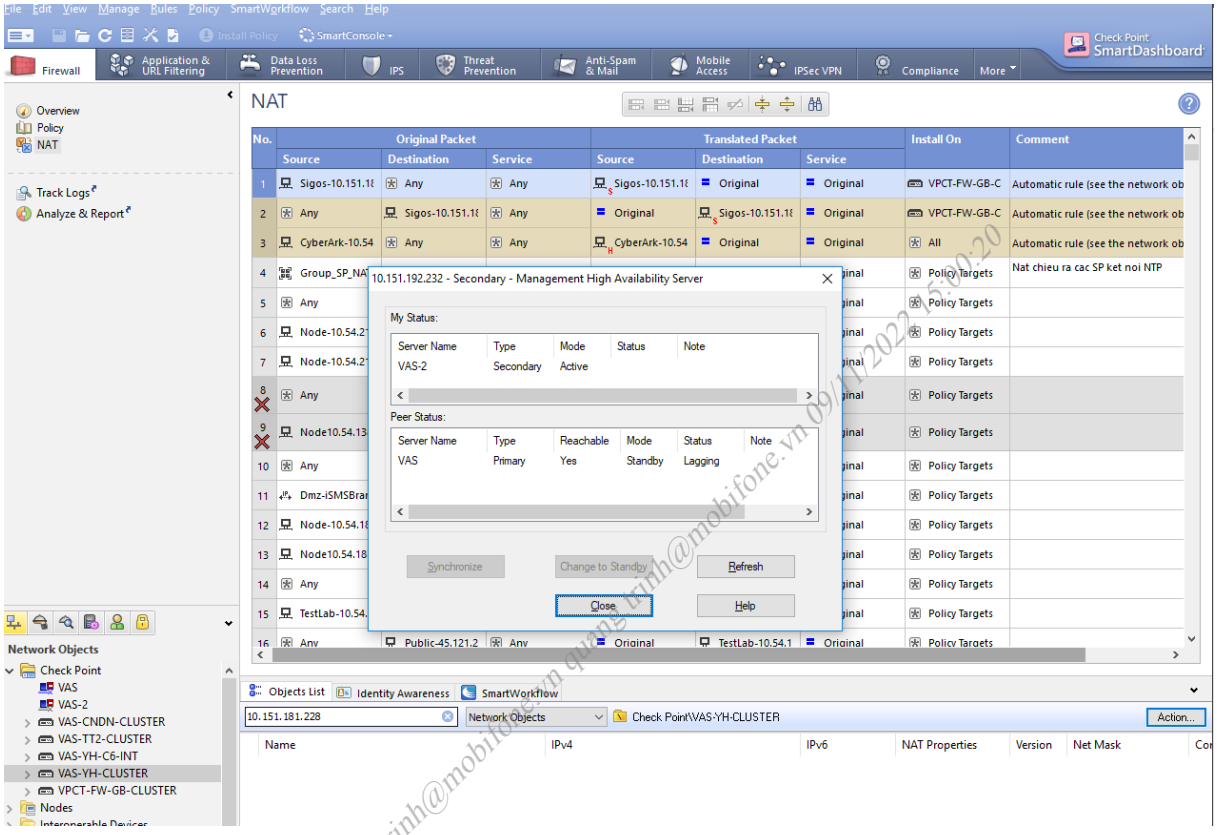


4. Đồng bộ trạng thái, đồng bộ đối tượng các Security Gateway

- Trên *Smart Dashboard → Click Policy → Management High Avaibility →*

Click Synchronize: Đồng bộ trạng thái, đồng bộ đối tượng, đồng bộ chính sách …

Click Change to Standby: chuyển đổi trạng thái active, standby giữa các security gateway



II. Tài liệu vận hành khai thác thiết bị Router Cisco ASR9000.

1. Backup cấu hình

- Đăng nhập vào thiết bị ASR9000, thực hiện các câu lệnh sau:

RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02#show run

Fri Aug 30 16:19:53.825 GMT

Building configuration...

!! IOS XR Configuration 5.3.4

!! Last configuration change at Thu Aug 29 09:07:44 2019 by hungpp

!

service unsupported-transceiver

hostname ASR9K-VAS-YHA-02

clock timezone GMT 7

```
logging trap debugging
logging 10.54.16.4 vrf default severity info port default
logging 10.54.24.210 vrf default severity info port default
logging 10.151.192.203 vrf default severity info port default
logging source-interface GigabitEthernet0/0/0/1
telnet vrf default ipv4 server max-servers 10
```

```
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02#show ip int brief
Fri Aug 30 16:20:53.160 GMT
Interface                  IP-Address      Status          Protocol Vrf-Name
BVI7                       10.54.24.133    Up              Up       default
BVI11                      10.54.24.245    Up              Up       default
BVI13                      10.54.24.150    Up              Up       default
BVI25                      10.54.24.229    Up              Up       default
Bundle-Ether2              unassigned      Up              Up       default
Bundle-Ether5              10.54.24.6      Up              Up       default
Bundle-Ether6              unassigned      Up              Up       default
```

```
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02#show interfaces description
Fri Aug 30 16:21:38.922 GMT
Interface      Status     Protocol    Description
--------------------------------------------------------------------------------
BV7            up         up
BV11           up         up
BV13           up         up
BV25           up         up
BE2            up         up         CONNECT TO ASR9K-VAS-YHA-01
BE2.1          up         up
```


2. Khai báo kết nối mới

- Thực hiện chuẩn bị hạ tầng vật lý, đi dây mạng giữa các thiết bị và hướng kết nối tới thiết bị khác.
- Trên interface, cấu hình các lệnh sau:

```
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02#show ru interface g0/0/0/4
```

```
Fri Aug 30 16:23:59.213 GMT
interface GigabitEthernet0/0/0/4
description CONNECT TO LMS-VAS-YHA-01
ipv4 address 10.54.24.209 255.255.255.252
flow ipv4 monitor monitor1 sampler sample1 ingress
!
```


3. Khai báo route

- Static route:

  Thực hiện các lệnh sau:

```
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02(config)#router static
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02(config-static)#address-family ipv4 unicast
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02(config-static)#10.151.181.0/24 10.54.20.1
RP/0/RSP0/CPU0:ASR9K-VAS-YHA-02(config-static)#commit
```

- Quảng bá thông qua OSPF:

  Thực hiện thêm các prefix list vào router ospf để quảng bá.

```
!
prefix-set static-ospf
  10.54.2.0/23 le 32,
  10.54.4.0/22 le 32,
  10.54.8.0/21 le 32,
  10.54.16.0/20 le 32
end - set
```

4. Khai báo tài khoản quản trị

III. Tài liệu vận hành khai thác thiết bị CoreSwitch 6509.

- Thiết bị switch đáp ứng các cấu hình sau:

STT	Nội dung cần đáp ứng
1	Kiểm tra tên và thông số cơ bản cho thiết bị
2	Kiểm tra Banner truy cập các thiết bị, các thông tin gồm: cảnh báo, thông tin cần liên hệ với quản trị thiết bị
3	Kiểm tra cấu hình xác thực user qua hệ thống xác thực tập trung
4	Kiểm tra các tài khoản mặc định của thiết bị, loại bỏ các tài khoản không sử dụng
5	Kiểm tra cấu hình log local, lưu log về hệ thống Syslog tập trung (SIEM)
6	Kiểm tra cấu hình an toàn cho SNMP, giám sát tập trung (Polestar)
7	Kiểm tra địa chỉ IP được phép quản lý thiết bị
8	Kiểm tra giao thức truy cập VTY: chỉ cho phép qua SSHv2 hoặc https2, loại bỏ truy cập qua http
9	Kiêm tra khai báo địa chỉ quản trị cho switch access
10	Kiểm tra địa chỉ IP cho Interface Loopback (Coreswitch, router)
11	Kiểm tra thời gian Idle Timeout: không vượt quá 15 phút
12	Kiểm tra cấu hình đồng bộ thời gian
13	Kiểm tra bảo mật, chống DHCP snooping (tránh cấp phát DHCP từ thiết bị ngoài)
14	Kiểm tra cấu hình các giao thức Spanning Trê (BPDU Guard, Root Guard …) tránh loop layer 2
15	Kiểm tra cấu hình port-security (tùy chọn, có thể cấu hình tùy theo nhu cầu của đơn vị)

IV. Tài liệu vận hành khai thác thiết bị Switch Aceess.

- Thiết bị switch đáp ứng các cấu hình sau:

STT	Nội dung cần đáp ứng
1	Kiểm tra tên và thông số cơ bản cho thiết bị
2	Kiểm tra Banner truy cập các thiết bị, các thông tin gồm: cảnh báo, thông tin cần liên hệ với quản trị thiết bị
3	Kiểm tra cấu hình xác thực user qua hệ thống xác thực tập trung
4	Kiểm tra các tài khoản mặc định của thiết bị, loại bỏ các tài khoản không sử dụng
5	Kiểm tra cấu hình log local, lưu log về hệ thống Syslog tập trung (SIEM)
6	Kiểm tra cấu hình an toàn cho SNMP, giám sát tập trung (Polestar)
7	Kiểm tra địa chỉ IP được phép quản lý thiết bị
8	Kiểm tra giao thức truy cập VTY: chỉ cho phép qua SSHv2 hoặc https2, loại bỏ truy cập qua http
9	Kiêm tra khai báo địa chỉ quản trị cho switch access
10	Kiểm tra địa chỉ IP cho Interface Loopback (Coreswitch, router)
11	Kiểm tra thời gian Idle Timeout: không vượt quá 15 phút
12	Kiểm tra cấu hình đồng bộ thời gian
13	Kiểm tra bảo mật, chống DHCP snooping (tránh cấp phát DHCP từ thiết bị ngoài)
14	Kiểm tra cấu hình các giao thức Spanning Trê (BPDU Guard, Root Guard …) tránh loop layer 2
15	Kiểm tra cấu hình port-security (tùy chọn, có thể cấu hình tùy theo nhu cầu của đơn vị)

PHỤ LỤC 02. DANH SÁCH THIẾT BỊ MẠNG BẢO MẬT TẠI TRUNG TÂM

STT	Chủng loại	Tên thiết bị	Vender	Vị trí
01	Firewall	VAS-FW-YH-01	Checkpoint Power – 1 15400	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		VAS-FW-YH-02	Checkpoint Power – 1 15400	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		MDS-FG-1101-01-YHA	Fortigate 1101E	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		MDS-FG-1101-02-YHA	Fortigate 1101E	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		MVAS-FG-1101-01-HCM	Fortigate 1101E	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		MVAS-FG-1101-02-HCM	Fortigate 1101E	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		VAS-FW-GB-01	Checkpoint Power – 1 5070	Tầng 5 – Tòa nhà MobiFone Giáp Bát
		VAS-FW-GB-02	Checkpoint Power – 1 5070	Tầng 5 – Tòa nhà MobiFone Giáp Bát
		VAS-FW-DN01	Checkpoint Power – 1 5070	Tầng 4 – Tòa nhà MobiFone An Đồn
		VAS-FW-DN02	Checkpoint Power – 1 5070	Tầng 4 – Tòa nhà MobiFone An Đồn
		VAS-TT2-FW01	Checkpoint Power – 1 9070	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		VAS-TT2-FW02	Checkpoint Power – 1 9070	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		VAS-TT2-FW02	Checkpoint Power – 1 5070	Thiết bị cũ - Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		VAS-TT2-FW02	Checkpoint Power – 1 5070	Thiết bị cũ - Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh

02	Switch Core	VSS6509_YH_01	Cisco 6509	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		VSS6509_YH_02	Cisco 6509	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		CS6509_GBT_01	Cisco WS-C6509-E	Tầng 5 – Tòa nhà MobiFone Giáp Bát
		CS6509_GBT_02	Cisco WS-C6509-E	Tầng 5 – Tòa nhà MobiFone Giáp Bát
		C7606-CRBT-GW-01	CISCO 7606	Tầng 3 – Tòa nhà MobiFone Giáp Bát
		C7606-CRBT-GW-02	CISCO 7606	Tầng 3 – Tòa nhà MobiFone Giáp Bát
		SW6509-ĐNA-01	Cisco WS-C6509-E	Tầng 4 – Tòa nhà MobiFone An Đồn
		SW6509-ĐNA-02	Cisco WS-C6509-E	Tầng 4 – Tòa nhà MobiFone An Đồn
		SW6509-VASHCM-L01	Cisco 6509	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		SW6509-VASHCM-L02	Cisco 6509	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
03	Switch Access	SW_Acc_YH_T4_01	Cisco 3560	Tầng 4 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T4_03	Cisco 3560	Tầng 4 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_02	cisco WS-C3560G-48TS	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_03	cisco WS-C3560G-48TS	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_04	cisco WS-C3560G-48TS	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_05	cisco WS-C3560X-48	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_06	cisco WS-C3560X-48	Tầng 6 – Tòa nhà MobiFone Yên Hòa

		SW_Acc_YH_T6_07	cisco WS-C3560X-48	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_08	cisco WS-C3560X-48	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_09	cisco WS-C3560X-48	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_10	cisco WS-C3560X-48	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_SP_01	cisco WS-C3560-48TS	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_YH_T6_SP_02	cisco WS-C2960-24TC-S	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		SW_Acc_GBT_T5_01	cisco WS-C3560G-48TS	Tầng 5 – Tòa nhà MobiFone Giáp Bát
		SW_Acc_GBT_T5_02	cisco WS-C3560G-48TS	Tầng 5 – Tòa nhà MobiFone Giáp Bát
		SW_Acc_GBT_T3_01	cisco WS-C3560X-48	Tầng 3 – Tòa nhà MobiFone Giáp Bát
		SW_Acc_GBT_T2_01	cisco WS-C3560G-48TS	Tầng 2 – Tòa nhà MobiFone Giáp Bát
		VAS_C_SW_DN01	cisco WS-C2960-24TC-S	Tầng 4 – Tòa nhà MobiFone An Đồn
		VAS_C_SW_DN02	cisco WS-C2960-24TC-S	Tầng 4 – Tòa nhà MobiFone An Đồn
		SW3560 -CNHCM	Cisco 3560	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		SW3560-VASHCM-L01	Cisco 3560	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		SW3560-VASHCM-L10	Cisco 3560	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		SW3560-VASHCM-SP	Cisco 3560	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
04	Router Core	ASR9K-VAS-YHA-01	ASR9K	Tầng 6 – Tòa nhà MobiFone Yên Hòa

		ASR9K-VAS-YHA-02	ASR9K	Tầng 6 – Tòa nhà MobiFone Yên Hòa
		ASR9K-VAS-GBT-01	ASR9K	Tầng 3 – Tòa nhà MobiFone Giáp Bát
		ASR9K-VAS-GBT-02	ASR9K	Tầng 3 – Tòa nhà MobiFone Giáp Bát
		ASR9K-DNG-01	ASR9K	Tầng 4 – Tòa nhà MobiFone An Đồn
		ASR9K-DNG-02	ASR9K	Tầng 4 – Tòa nhà MobiFone An Đồn
		ASR9K-VASHCM-01	ASR9K	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		ASR9K-VASHCM-02	ASR9K	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		RouterCP_7606_HN	Cisco 7606	Tầng 4 – Tòa nhà MobiFone Yên Hòa
		RouterCP_7606_HCM	Cisco 7606	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		Router_CP7613_YHA	Cisco 7613	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh
		Router_CP7613_HCM	Cisco 7613	Lầu 1 – Tòa nhà C30 MobiFone Thành phố Hồ Chí Minh

PHỤ LỤC 03: BIỂU MẪU ĐÁNH GIÁ HỆ THỐNG

PHIẾU ĐÁNH GIÁ HỆ THỐNG

Đơn vị đánh giá: ……. .....

Hệ thống: ....

Ngày ứng dụng đưa vào hệ thống: .....Ngày đánh giá: .....….....

1. Nội dung đánh giá:

a. Mức độ ổn định của hệ thống:

- Không có lỗi:.....
- Có lỗi xảy ra:
  + Tần suất lỗi: .....
  + Lỗi lặp lại: .....
  + Mô tả lỗi: .....

b. Khả năng đáp ứng của hệ thống

+ Số lượng giao dịch trong giờ cao điểm .....
+ Số lượng giao dịch ứng dụng đáp ứng: .....
+ Tốc độ xử lý của 1 giao dịch: .....

c. Công cụ giám sát:.....

d. Công cụ hỗ trợ xử lý:.....

2. Tài liệu vận hành khai thác

+ Các hướng dẫn vận hành khai thác: .....

+ Hướng dẫn sử dụng công cụ giám sát:.....

+ Hướng dẫn sử dụng công cụ hỗ trợ xử lý lỗi: .....

+ Tài liệu mô tả lỗi (Nếu có trong quá trình triển khai) :.....

3. Kết luận

PHỤ LỤC 04. CÁC BIỂU MẪU ĐĂNG KÝ

Mẫu 1:

PHIẾU ĐỀ NGHỊ
CẤP PHÁT/THU HỒI ĐỊA CHỈ IP CHO MÁY TÍNH CÁ NHÂN

1. Căn cứ:……
2. Ngày đăng ký:…….
3. Đơn vị: Trung tâm Dịch vụ Số MobiFone
4. Phòng/ban:……
5. Họ tên người đề nghị:……
6. Thông tin máy tính người được cấp phát/thu hồi:

Họ tên	PC name	MAC Address	Email

7. Mục đích: (cấp phát/thu hồi) địa chỉ IP
8. Thời hạn sử dụng:…….
9. Mức độ ưu tiên cần giải quyết:

☐ Rất Khẩn ☐ Khẩn ☐ Bình thường

Tôi xin cam kết và hoàn toàn chịu trách nhiệm về việc sử dụng địa chỉ IP theo quy định của Trung tâm Dịch vụ Số MobiFone.

Người đề nghị **Lãnh đạo đơn vị**

MẪU 2:

PHIẾU ĐỀ NGHỊ

ĐĂNG KÝ/LOẠI BỎ KẾT NỐI QUA FIREWALL

1. Ngày:.....
2. Đơn vị: .....
3. Người đề nghị….....
4. Yêu cầu

☐ Khai báo kết nối ☐ Loại bỏ kết nối

5. Thông tin truy cập

STT	Địa chỉ IP/subnet mask nguồn	Địa chỉ IP/subnet mask đích	Dịch vụ (port)	Thời gian truy cập/huỷ bỏ	Lý do

6. Mức độ ưu tiên cần giải quyết:

☐ Rất khẩn ☐ Khẩn ☐ Bình thường

Người đề nghị **Lãnh đạo đơn vị ký duyệt**

MẪU 3:

PHIẾU ĐỀ NGHỊ
ĐĂNG KÝ / LOẠI BỎ ACCOUNT TRUY CẬP VPN

1. Ngày: .....
2. Đơn vị: .....
3. Người đề nghị.....
4. Yêu cầu:

☐ Thêm ☐ Xóa ☐ Reset password

☐ Đổi tên tài khoản:

6. Được sử dụng đến ngày:
7. Tài nguyên cần truy cập

STT	IP	Port	Mô tả

Thời gian đăng ký/loại bỏ:

8. Mức độ ưu tiên cần giải quyết:

☐ Rất khẩn ☐ Khẩn ☐ Bình thường

Người đề nghị **Lãnh đạo đơn vị**