

Đại học SPKT TP.HCM



HCMUTE

MÔ HÌNH HỆ THỐNG CNTT CHO DOANH NGHIỆP

Tài liệu quản trị

Version 1.1
11/2020

CHUẨN BỊ CHO: ĐẠI HỌC SPKT
BỞI: TECHHORIZON

Mục lục

1	
1	TỔNG QUAN 5
1.1	Giới thiệu 5
1.2	Mô tả kiến trúc hạ tầng CNTT của doanh nghiệp 5
1.3	Các nhà cung cấp 6
1.3.1	Fortinet 6
1.3.2	Array Network 7
1.3.3	Alied Telesis 9
1.3.4	ZyXEL 10
1.3.5	QNAP 12
2	CÁC THÀNH PHẦN CỦA GIẢI PHÁP 14
2.1	Hạ tầng mạng Access 14
2.1.1	Mô tả 14
2.1.2	Các thiết bị đầu tư 14
2.2	Hạ tầng Mạng Core 16
2.2.1	Mô tả 16
2.2.2	Các thiết bị đầu tư 16
2.3	Hạ tầng bảo mật mạng biên 17
2.3.1	Mô tả 17
2.3.2	Các thiết bị đầu tư 17
2.4	Hạ tầng bảo mật mạng nội bộ 18
2.4.1	Mô tả 18
2.4.2	Các thiết bị đầu tư 19
2.5	Hạ tầng Ứng dụng 20
2.5.1	Mô tả 20
2.5.2	Các thiết bị đầu tư 20
2.6	Hạ tầng Quản lý 22
2.6.1	Mô tả 22
2.6.2	Các thiết bị đầu tư 23
2.7	DR-DC 26
3	CÁC NỘI DUNG THỰC HÀNH LAB 28
3.1	Hệ thống Network 28
3.1.1	Access Network 28
3.1.2	Core Network 28
3.2	Hệ thống bảo mật 29
3.2.1	Bảo mật mạng biên 29
3.2.2	Bảo mật mạng nội bộ 29
3.2.3	Bảo mật Mail 29
3.2.4	Bảo mật Web 29
3.2.5	Cân bằng tải Ứng dụng 30

3.2.6	Bảo mật Endpoint.....	30
3.2.7	Hệ thống xác thực tập trung	30
3.2.8	Hệ thống phòng chống APT.....	30
3.3	Hệ thống quản lý.....	30
3.3.1	Hệ thống quản lý các thiết bị Firewall	30
3.3.2	Hệ thống quản lý SIEM	31
3.3.3	Hệ thống lưu trữ NAS.....	31
3.4	DR-DC.....	31
3.4.1	Khả năng đồng bộ.....	31
3.4.2	Khả năng dự phòng.....	31
4	MÔ HÌNH KẾT NỐI VẬT LÝ.....	32
4.1	Các thiết bị trung tâm	32
4.2	Các thiết bị trong vùng Server	33
4.3	Các thiết bị chính tại Site DR	33
4.4	Các thiết bị khác	34
4.4.1	Vùng kết nối WAN đồng bộ Site to Site	34
4.4.2	Vùng kết nối WAN DR-DC	34
4.4.3	Thiết bị FortiSandbox.....	35
5	QUY HOẠCH HỆ THỐNG.....	36
5.1	Quy hoạch IP và Kết nối.....	36
5.2	Quy hoạch Port cho hạ tầng Access Switch	38
5.2.1	Quy hoạch Port trên Switch Access dành cho hệ WAN và Server	38
5.2.2	Quy hoạch Port trên Switch Access dành cho hệ User và quản trị	39
5.2.3	Quy hoạch Port trên Switch Access dành cho Site DR	39
5.3	IP Quản trị hệ thống	40
6	CÁC HƯỚNG DẪN.....	41
6.1	Hướng dẫn khôi phục hệ thống.....	41
6.1.1	Zyxel.....	42
6.1.2	Engenius	43
6.1.3	Allied Telesis	47
6.1.4	Các thiết bị Fortigate.....	49
6.1.5	Thiết bị FortiWeb	51
6.1.6	Thiết bị FortiAuthenticator	51
6.1.7	Thiết bị FortiManager.....	52
6.1.8	Thiết bị QNAP	54
6.1.9	Thiết bị FortiMail	55
6.1.10	Thiết bị FortiSandbox.....	57
6.1.11	Thiết bị FortiEMS	58
6.1.12	Thiết bị FortiSIEM	59
6.1.13	Thiết bị Array Network	59
6.2	Hướng dẫn vận hành các máy chủ ảo	60
6.2.1	Thông tin truy cập vào các thiết bị bên trong VM ESX:	60
6.2.2	Hướng dẫn sử dụng VM ESXi	61
7	SƠ ĐỒ BỐ TRÍ RACK.....	64

7.1	Nguyên lý.....	64
7.2	Ảnh thực tế.....	65

1 Tổng quan

1.1 Giới thiệu

Trong xu thế hiện tại, việc ứng dụng CNTT trong môi trường Doanh nghiệp ngày càng đóng vai trò quan trọng. Do đó nhu cầu về nhân sự CNTT cũng ngày một đòi hỏi gắt gao hơn về chất lượng, điều này cho thấy vấn đề giáo dục đào tạo cho sinh viên tại các trường Đại học/Cao Đẳng ngày càng được quan tâm nhiều hơn, mục tiêu là thế hệ sinh viên trẻ mới ra trường ít nhất phải có các kiến thức nền tảng để nhanh chóng đáp ứng được yêu cầu về công việc khi gia nhập môi trường làm việc thực tế tại các Doanh nghiệp, đặc biệt là các Doanh nghiệp lớn, Doanh nghiệp nước ngoài...

Bên cạnh các kiến thức học trong trường, việc cho các sinh viên tiếp cận thực tế với các hệ thống CNTT của doanh nghiệp cũng là một bước quan trọng để nâng cao cái nhìn của các em về những gì đã được học, đã được nghe nói đến. Điều này, thực tế các em khó tiếp cận, có chăng chỉ được tiếp xúc ít nhiều qua thời gian thực tập.

Thể theo nhu cầu đó của nhà trường, là nhà phân phối rất nhiều các giải pháp chuyên nghiệp dành cho hạ tầng CNTT, Tech Horizon mong muốn mang lại một mô hình giải pháp thực tế, thu nhỏ, dành cho các Sinh viên chuyên ngành Mạng máy tính, để nhà trường có thể từ đây, thực hiện các giáo trình chuyên môn để các em có cơ hội tiếp cận sâu hơn, thực tế hơn với các hệ thống mà một doanh nghiệp hiện đại đang có, nâng cao chất lượng đào tạo của nhà trường cũng như giúp các em có được nhiều cơ hội hơn sau khi ra trường.

1.2 Mô tả kiến trúc hạ tầng CNTT của doanh nghiệp

Kiến trúc CNTT cho doanh nghiệp gồm các Vùng thành phần hệ thống như sau: Vùng Hạ tầng (infrastructure domain), Vùng dữ liệu (data domain), Vùng ứng dụng (Application domain), Vùng người dùng (user domain), và Vùng bảo mật (security domain).

Các vùng thành phần hệ thống được định nghĩa với các vai trò và chức năng khác nhau, nhưng liên quan mật thiết với nhau, tạo thành một khối kiến trúc CNTT vững chắc cho doanh nghiệp, cụ thể như sau:

- **Vùng Hạ tầng – (Infrastructure Domain):** Bao gồm các phân hệ chức năng như Phân hệ mạng nội bộ/mạng khuôn viên/wireless; Phân hệ mạng biên gồm DMZ, Wan, Internet, cổng dịch vụ; Phân hệ chuyển mạch lõi; Phân hệ trung tâm dữ liệu; và Phân hệ dịch vụ hạ tầng.
- **Vùng Dữ liệu – (Data Domain):** Gồm các phân hệ Dữ liệu con cho doanh nghiệp gồm Dữ liệu hệ thống; dữ liệu bán hàng, dữ liệu khách hàng, dữ liệu nhân viên (kế toán, các phòng ban, v.v...). Hệ thống dữ liệu được xây dựng sao cho việc lưu trữ, truy xuất, dự phòng và sử dụng hiệu quả phù hợp với cơ cấu và chính sách của doanh nghiệp.
- **Vùng Ứng dụng – (Application Domain):** Thể hiện nhiều phân hệ ứng dụng khác nhau như ứng dụng nền tảng (Web, Mail, IM, v.v...), ứng dụng quản lý (kế toán, tài sản, v.v...), ứng dụng dịch vụ (dịch vụ bán hàng, dịch vụ thoại truyền hình, v.v...). Các ứng dụng này sẽ được xem xét và phát triển chi tiết, tạo thành một hệ thống ứng dụng đầy đủ, hiệu quả cho hoạt động của doanh nghiệp.

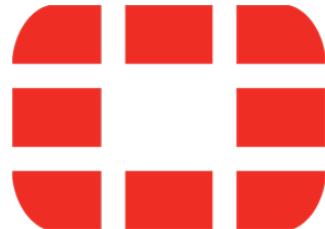
- **Vùng Bảo mật – (Security Domain):** Đây là Vùng giữ vai trò quan trọng, có quan hệ mật thiết với tất cả các Vùng khác trong kiến trúc tổng thể. Vùng bảo mật gồm nhiều phân hệ bảo mật thực hiện các cơ chế bảo mật, chính sách bảo mật nhằm nâng cao tính toàn vẹn dữ liệu thường xuyên được tương tác, đồng thời hạn chế tối đa các rủi ro về an toàn hệ thống thông tin cho toàn doanh nghiệp.

1.3 Các nhà cung cấp

1.3.1 Fortinet

Fortinet được thành lập trong năm 2000 bởi Ken Xie – Trước đây, ông Ken Xie là sáng lập viên, đồng chủ tịch và CEO của hãng bảo mật nổi tiếng NetScreen

- Văn phòng chính ở Sunnyvale, CA.
- Số lượng nhân viên hiện tại trên 1,500 nhân viên kỹ thuật và nghiên cứu phát triển
- Có trên 30 văn phòng ở các châu Mỹ, châu Á và châu Âu
- Tập trung chính vào các giải pháp bảo mật.
- Là nhà tiên phong trong các hệ thống antivirus chạy trên ASIC, đảm bảo tính bảo vệ mạng theo thời gian thực
- Đứng đầu danh sách đánh giá của IDC và Gartner đối với dòng sản phẩm UTM
- Có năng lực tài chính mạnh, phát triển nhanh.



Là công ty duy nhất đạt được 8 chứng nhận của ICSA Lab và 2 chứng chỉ NSS Lab

Các sản phẩm bảo mật của Fortinet gồm :

Fortigate Firewall : thiết bị bảo mật tường lửa + VPN, có thể tích hợp các tính năng Antivirus, IPS, AntiSpam, Web filtering, Application Control, Data Leak Prevention ...

FortiMail : thiết bị chuyên dùng để bảo vệ riêng hệ thống email khỏi Antivirus/Worm/Spyware và AntiSpam

FortiAnalyzer : thiết bị ghi log tập trung và phân tích log, scan hệ thống để tìm ra lỗ hổng

FortiManager : thiết bị quản lý tập trung thiết bị Fortigate và FortiClient, cho phép người quản trị quản lý, cấu hình, update và áp dụng chính sách bảo mật chung cho tất cả các thiết bị Fortigate & FortiClient trong toàn hệ thống

FortiClient : phần mềm personal firewall + VPN cho người sử dụng di động. Có thể mua thêm license để có thêm các tính năng Antivirus, AntiSpam & Web filtering

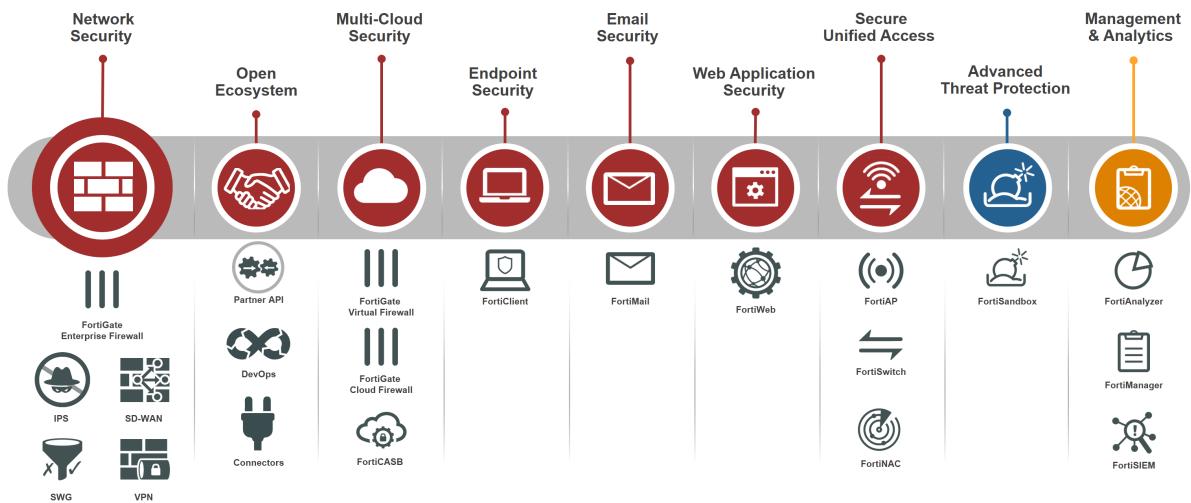
Fortiguard subscription service : license đăng ký sử dụng và update các tính năng Antivirus, IPS, AntiSpam và Web filtering. License có thể mua mới hàng năm hoặc nhiều năm

Forticare service : dịch vụ hỗ trợ kỹ thuật, gia tăng thời gian bảo hành của sản phẩm cũng như update các OS/firmware mới nhất cho sản phẩm. Dịch vụ này có thể mua hàng năm hoặc nhiều năm.

Ngoài ra, còn rất nhiều giải pháp bảo mật quan trọng khác mà Fortinet đang cung cấp, là thương hiệu bảo mật có dải sản phẩm rộng nhất hiện nay trên thị trường :

The Broadest Security Portfolio in the Industry

Built From The Ground Up To Deliver True Integration End To End



1.3.2 Array Network

Array Network được thành lập năm 2000 tại Milpitas, CA, USA, là công ty chuyên về lĩnh vực Application Delivery, với các sản phẩm :

- APV Series :** là thiết bị Application Delivery Controller, tích hợp các tính năng hiện đại : Link Load Balancing, Server Load Balancing, Global Load Balancing, SSL Accelerating..., mang lại hiệu quả trong việc cân bằng tải giữa các đường truyền/Server, đảm bảo các cơ chế dự phòng, nâng cao tốc độ xử lý đối với các dịch vụ đòi hỏi độ bảo mật cao...
- aCelebra Series :** thiết bị WAN Optimize chuyên dụng, hỗ trợ tăng tốc kết nối, đảm bảo hiệu quả đường truyền trong mô hình mạng WAN, giúp nâng cao trải nghiệm người dùng trong khi vẫn tiết kiệm được kinh phí đầu tư cho băng thông kết nối giữa các site với nhau.
- AG Series:** là thiết bị Secure Gateway, hỗ trợ mô hình doanh nghiệp với kết nối SSL VPN với số lượng lớn User, đồng thời thiết bị còn cho phép quản lý/kiểm soát toàn bộ các thiết bị di động (BYOD), với các tính năng ưu việt, mang lại hiệu quả bảo mật tối đa cho hệ thống mạng bên trong cũng như người dùng đầu cuối



Kiến trúc Speed Core của Array Network:

Là một kiến trúc mở 64-bit, được xây dựng chuyên biệt nhằm nâng cao khả năng xử lý đa nhân của các nền tảng phần cứng lẫn ảo hóa



- Cho phép doanh nghiệp có thể quản lý tập trung toàn bộ hệ thống, mang lại hiệu quả tốt nhất đối với các tác vụ đòi hỏi cao về cấu hình phần cứng (CPUs), trong khi vẫn tối ưu được trải nghiệm người dùng.
- Được tích hợp sẵn trong tất cả các sản phẩm của Array Network

Server Load Balancing

Server Load Balancing là tính năng phân phối tải kết nối của User từ bên ngoài vào nhiều Server dịch vụ bên trong.

Tính năng này giải quyết được các vấn đề như sau :

- Tránh tình trạng quá tải khi số lượng kết nối của User bên ngoài vào quá nhiều, 1 Server bên trong không đủ khả năng phục vụ
- Tránh tình trạng fail dịch vụ khi Server bên trong bị sự cố
- Giảm tải cho Server khi chạy dịch vụ, các traffic sẽ được phân phối đến nhiều Server khác nhau chạy cùng một loại dịch vụ (Web/Email/Database/FTP...), nhằm tối ưu hoạt động và tăng tuổi thọ của các Server

Tính năng Server Load Balancing của dòng sản phẩm APV được tích hợp các tính năng vượt trội:

Layer 2-3 load balancing

Cân bằng tải dựa trên IP/MAC address

Round robin, persistent IP (source + destination), tính năng return to sender

Layer 4 load balancing

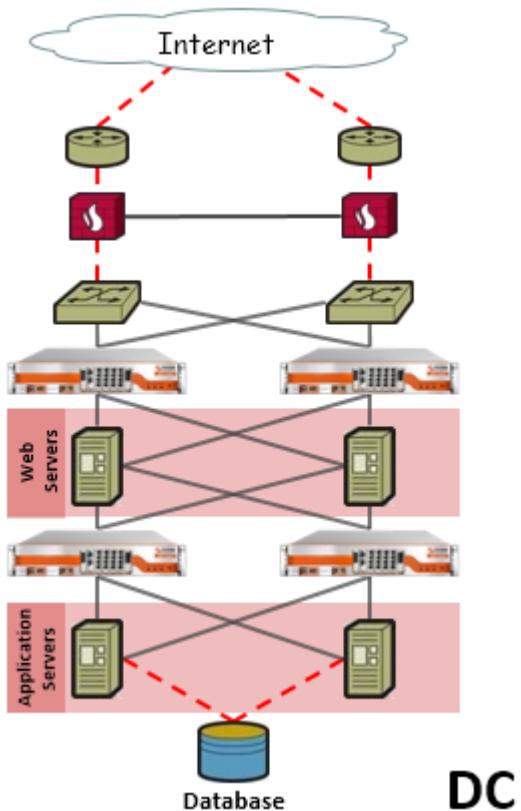
Cân bằng tải traffic dựa vào các port dịch vụ TCP, TCPS, UDP

Hỗ trợ các giao thức : Round robin, weighted round robin, least connections, shortest response methods, Persistent IP, hash IP, consistent hash IP, persistent IP + port, port range policies

Single port & composite port TCP applications

Hỗ trợ RADIUS & DNS server load balancing

Layer 7 application load balancing



DC

Hỗ trợ Load Balancing theo các ứng dụng : HTTP/HTTPS/FTP/FTPS/SIP/RTSP/RDP protocol balancing

Hỗ trợ các ứng dụng Web-based ERP/CRM

1.3.3 Allied Telesis

Allied Telesis là doanh nghiệp lâu đời và uy tín của Nhật Bản được thành lập từ tháng 3/1987 với số vốn điều lệ ban đầu đến 1 triệu Yen. Hơn 30 năm phát triển, Allied Telesis hôm nay trở thành một trong những nhà sản xuất hàng đầu thị trường về thiết bị truyền dẫn, giải pháp của Allied Telesis tập trung vào mạng và viễn thông trên nền IP từ Card mạng cho đến Media converter,

Router, Switch, Wireless và hệ thống quản lý cho các giải pháp này (network management system). Ngoài ra Allied Telesis còn hợp tác với nhiều nhà sản xuất khác để cung cấp các giải pháp cao cấp hơn như Extricom (Ixrael) chuyển cung cấp giải pháp Wireless quản lý tập trung; Root (Nhật Bản); Panasonic (Surveillance), v.v..

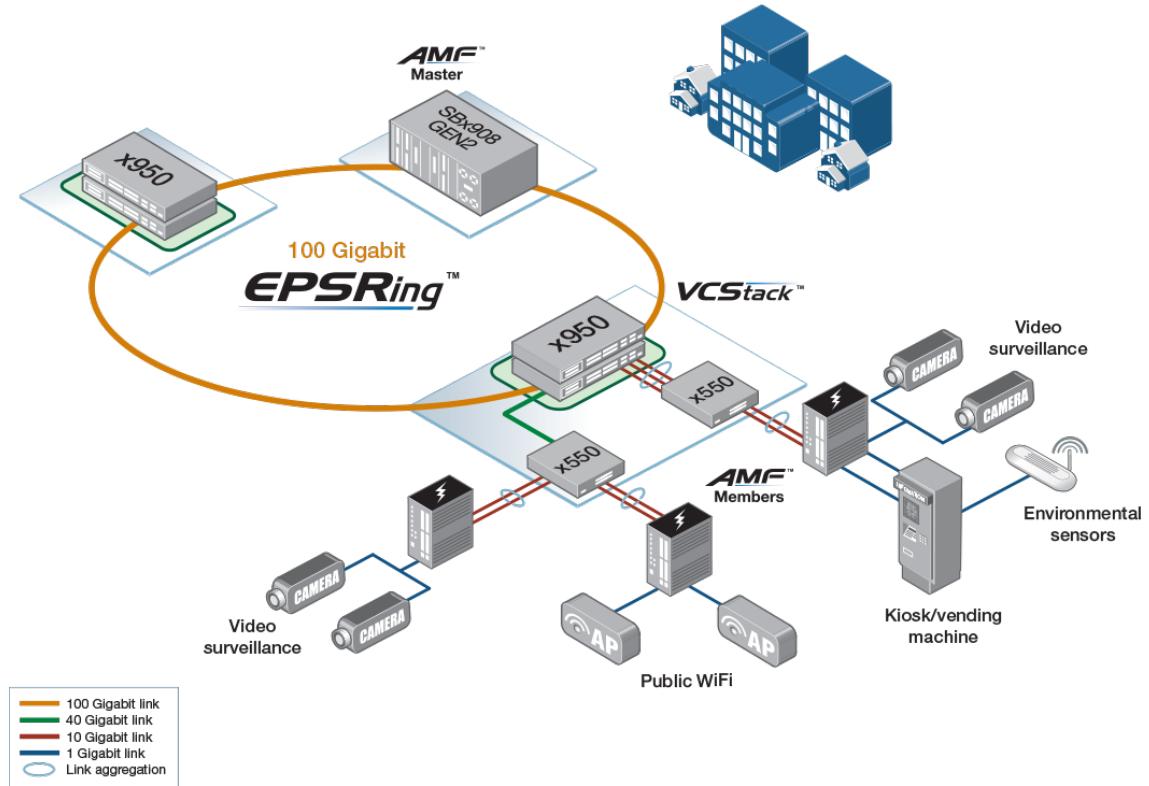
Allied Telesis đã từng giành được nhiều giải thưởng quan trọng như iCMG Architecture of Excellence, iCMG Architecture...

Thế mạnh của Allied Telesis là các dòng sản phẩm Switch, cung cấp các giải pháp hoàn chỉnh từ Unmanaged Switch cho đến Web Managed (WebSmart), Switch chuyên dụng cho công nghiệp, Layer2, Layer3, Advanced Layer 3 với khả năng chuyển mạch lên đến 1.92Tbs. Các sản phẩm của Allied Telesis luôn là các sản phẩm chất lượng cao, đã được kiểm định nghiêm ngặt theo tiêu chuẩn của Nhật Bản, đạt hiệu suất làm việc tối ưu, đáp ứng được tất cả các nhu cầu của khách hàng về truyền tải cho cả Media và Data với tốc độ và bảo mật cao nhất, đồng thời vẫn đảm bảo hiệu quả đầu tư với chi phí rất cạnh tranh.



Các sản phẩm của Allied Telesis được trang bị nhiều công nghệ hiện đại, tính năng hữu ích và tiện lợi cho người dùng cả về phần cứng lẫn phần mềm điều khiển và quản lý. Tại

Việt Nam, với bờ biển dài thị trường, hạ tầng quản trị mạng sử dụng thiết bị của Allied Telesis đã được đầu tư rất nhiều ở các dự án Chính Phủ và doanh nghiệp lớn trong và ngoài nước, cho mọi loại hình từ SMB, Enterprise, Bệnh viện, Khách sạn, Trường học...



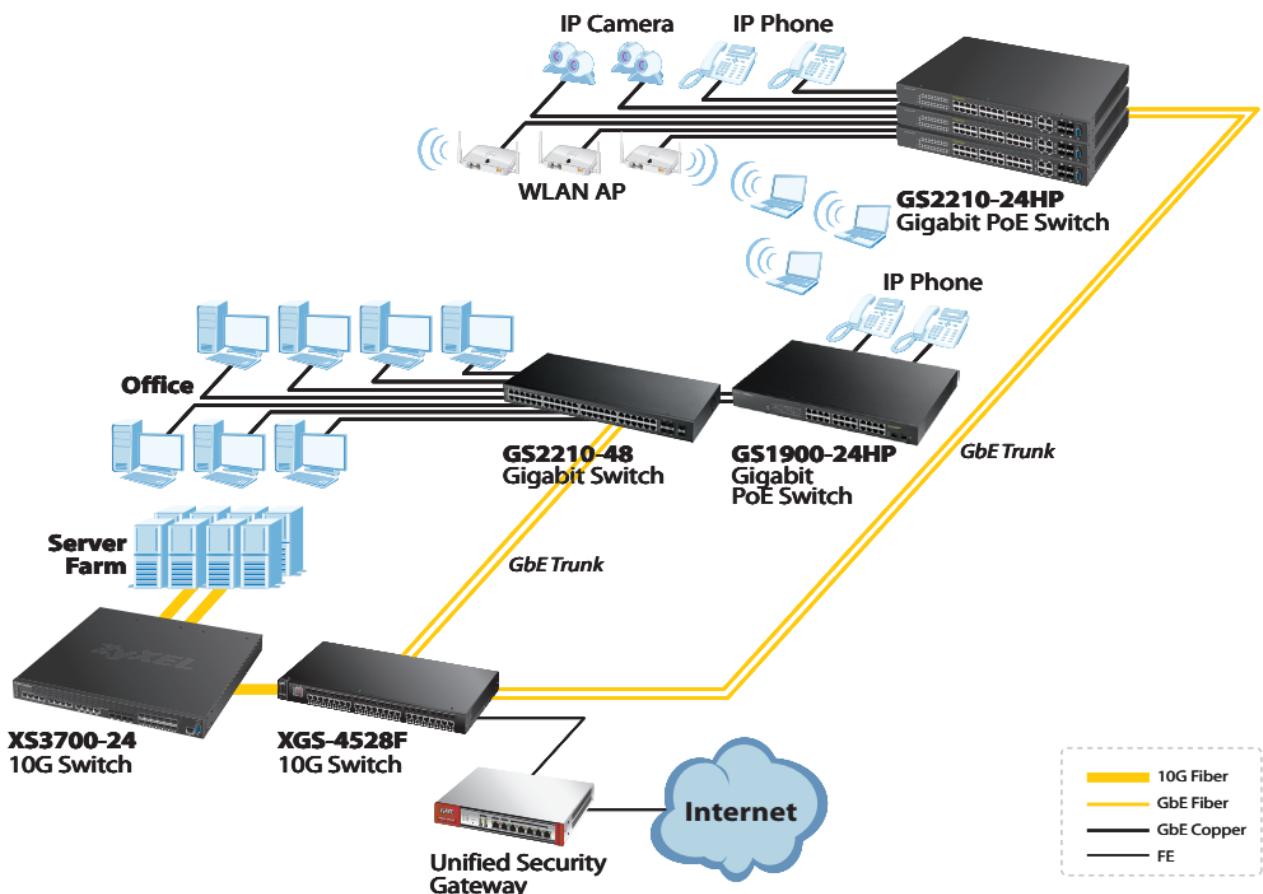
1.3.4 Zyxel

Tập trung vào đổi mới và hướng khách hàng làm trung tâm, Zyxel Communications Corp đã kết nối mọi người với internet trong gần 30 năm. Chúng tôi không ngừng thúc đẩy sự sáng tạo để đáp ứng các nhu cầu của khách hàng. Tinh thần này đã không hề thay đổi kể từ khi chúng tôi phát triển thiết bị tích hợp 3-trong-1 data/fax/voice đầu tiên trên thế giới vào năm 1992. Với khả năng thích ứng và đổi mới với công nghệ mạng giúp chúng tôi luôn đi đầu trong khả năng kết nối cho các công ty viễn thông/ nhà cung cấp dịch vụ, các doanh nghiệp và người dùng gia đình.

ZYXEL
Your Networking Ally

Chúng tôi đang xây dựng các hệ thống mạng cho tương lai, giúp khai phá tiềm năng của thế giới và đáp ứng nhu cầu của môi trường làm việc hiện đại; tạo năng lượng cho mọi người trong công việc, cuộc sống và vui chơi. Chúng tôi luôn sát cánh với khách hàng và các đối tác để chia sẻ các phương pháp mới để kết nối mạng và phát huy tối đa các khả năng của mình. Như người bạn trung thành, đồng minh mạnh mẽ, nguồn đáng tin cậy - Chúng tôi là **Zyxel, Your Networking Ally**.

Các giải pháp Zyxel Switch



Kết nối tốc độ cao

Thiết bị Switch Zyxel được thiết kế để cung cấp tốc độ cao trong hệ thống mạng và dành cho các ứng dụng cần lượng băng thông cao. Với công nghệ Gigabit Ethernet, Switch Zyxel cung cấp khả năng kết nối cho dữ liệu, ứng dụng voice, ứng dụng video. Thiết bị cũng có tính năng công kết nối 10G để dành cho việc kết nối với hệ thống máy chủ tốc độ cao.

Khả năng quản lý với nhiều lựa chọn

Thiết bị Switch Zyxel cung cấp nhiều lựa chọn trong việc quản lý và tính năng để triển khai một cách dễ dàng. Nhân viên IT có thể quản lý Switch Zyxel thông qua Web Gui, CLI hoặc SNMP. Quản lý qua giao diện Web dễ dàng đối với những người dùng không phải là kỹ thuật, trong khi đó việc quản lý qua CLI đòi hỏi người IT phải có những kinh nghiệm và kỹ năng nhất định. Với hệ thống hỗ trợ LLDP và LLDP-MED, Zyxel Switch cung cấp khả năng phát hiện tự động để dễ dàng trong việc triển khai thiết bị.

Power over Ethernet – PoE

Zyxel cung cấp một loạt các sản phẩm về Switch PoE nhằm giúp các doanh nghiệp dễ dàng hơn trong việc cài đặt cho WLAN, VoIP, và IP camera. Switch PoE Zyxel bao gồm các dòng unmanaged, smart managed và fully managed. Thiết bị được thiết kế với khả năng cung cấp PoE thông minh và tính năng quản lý công suất cấp để giúp các doanh nghiệp sử dụng một cách hiệu quả về mặt năng lượng và giúp tối ưu hóa dịch vụ.

PoE thông minh

Switch PoE Zyxel với công nghệ PoE thông minh giúp tự động phát hiện mức tiêu thụ của thiết bị cần PoE và chỉ cung cấp vừa đủ phần công suất thiết bị yêu cầu. Khi kích hoạt tính

năng này Switch PoE Zyxel sử dụng năng lượng một cách hiệu quả hơn và giúp cho doanh nghiệp tiết kiệm được một khoảng chi phí về điện năng.

Quản lý tập trung năng lượng

Switch PoE Zyxel cung cấp khả năng giám sát mức tiêu thụ năng lượng và cung cấp chính sách việc cấp phát năng lượng. Các tính năng giám sát và quản lý giúp cho người IT quản lý mức năng lượng của thiết bị một cách hiệu quả hơn và dễ dàng tối ưu hóa dịch vụ.

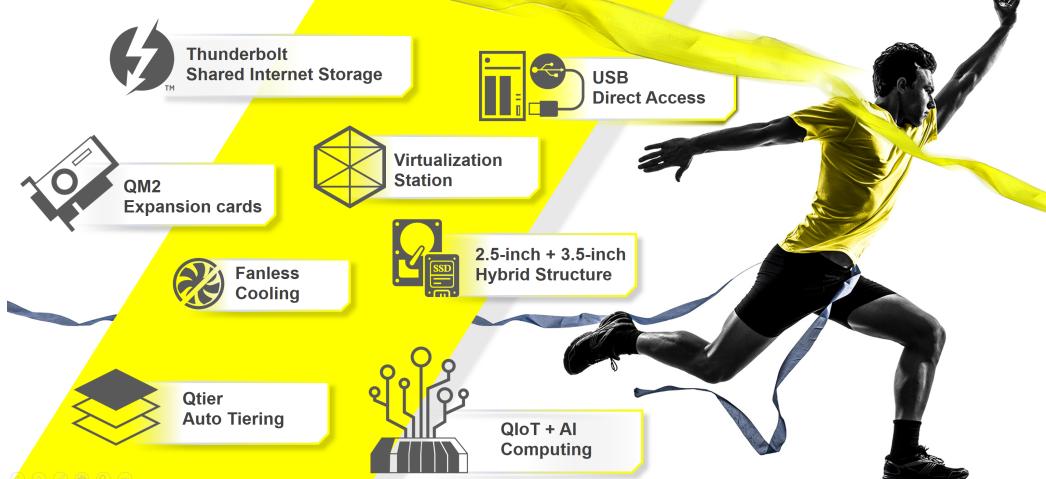
1.3.5 QNAP

QNAP® Systems được thành lập từ 2004, chuyên cung cấp các giải pháp giải pháp NAS cho phân khúc khách hàng từ SOHO, SMP, Enterprise và cả người dùng gia đình.



Giải pháp NAS là giải pháp chủ lực của QNAP, với các dòng sản phẩm phục vụ cho lưu trữ file, dự phòng, iSCSI, QvPC, ảo hóa, Container, IoT, đa phương tiện... Các hệ thống lưu trữ tiên tiến này hỗ trợ nhiều tính năng hiện đại ưu việt cùng với chủng loại sản phẩm đa dạng phù hợp với mọi quy mô, là một trong những lựa chọn có sức cạnh tranh trên thị trường hiện nay.

Leading the NAS Industry



QNAP từ lâu đã cam kết cung cấp các giải pháp về lưu trữ tốt nhất. Bên cạnh việc tối ưu hóa và cải tiến không ngừng về phần cứng, QNAP cũng đã đưa ra những cải tiến và thách thức mới trong lĩnh vực phần mềm và phát triển một loạt các giải pháp thông minh, toàn diện đẩy NAS vượt lên những giới hạn thông thường. QNAP ngày nay không chỉ là thiết bị lưu trữ để bảo vệ dữ liệu, sao lưu và phục hồi - nó còn là một nền tảng tích hợp cho nhu cầu cá nhân, gia đình và doanh nghiệp của bạn.

Với QNAP, hiệu quả làm việc được tăng lên đáng kể và giải trí kỹ thuật số chưa bao giờ thú vị hơn. Theo Gartner, một công ty nghiên cứu và tư vấn quốc tế, 10 xu hướng công nghệ hàng đầu từ năm 2016 chỉ ra rằng trong 20 năm tới, các đại lý tự động và thông minh sẽ tiếp tục cuộc cách mạng phát triển và mở rộng trong ứng dụng.

Giải pháp NAS

NAS là một hệ thống lưu trữ dựa trên cơ sở mạng hiện có và chỉ cho phép hệ thống lưu trữ dữ liệu thông qua hệ thống mạng. Những thiết bị NAS có tổng giá trị đầu tư thấp

nhưng thể hiện được những tính năng vượt trội như : hiệu suất, tính mềm dẻo và tính sẵn sàng cao của hệ thống.



Adding Storage Space

Không gian lưu trữ là quan trọng, đặc biệt là đối với những người đang nghĩ về nhu cầu tương lai của họ và địa chỉ máy chủ NAS cần cho một nhóm người dùng làm việc trong một văn phòng nhỏ. Đây là một cách hiệu quả hơn để cung cấp dung lượng lưu trữ cho mọi người và nhằm loại bỏ nhu cầu mua thêm ổ đĩa cứng riêng lẻ cho mỗi máy tính trên mạng.

Efficient Data Transfer and Reliable Network Access

Chỉ cần kéo và thả một tệp khá lớn vào thư mục mạng chia sẻ để phép bất kỳ máy tính nào khác được kết nối với máy chủ mạng truy cập vào dữ liệu đó. Máy tính trong một mạng chia sẻ có thể kết nối với máy chủ NAS chính hoặc không dây hoặc thông qua cáp ethernet. Điều này có thể thay đổi tốc độ truyền dữ liệu nào.

Ease of Accessibility from Multiple Locations

Theo cùng một dòng truyền dữ liệu, các máy chủ được nối mạng sẽ làm cho thông tin và các tệp có thể truy cập được từ nhiều vị trí khác nhau. Điều này có thể cực kỳ hiệu quả và hữu ích trong một môi trường văn phòng nhỏ, khi nhiều người cần tham khảo một tài liệu, hoặc thậm chí chỉnh sửa nó.

Sharing Capabilities

Một trong những lý do mà nhiều chủ nhà xem xét việc triển khai một Network Attached Server trong nhà của họ, là chia sẻ khả năng giải trí từ phòng này sang phòng khác. Nếu một người trong nhà có một đĩa CD trên máy tính của họ, nhưng họ muốn nghe nó trên máy tính gia đình trong phòng khách, một máy chủ NAS cho phép chức năng này.

Protecting Small Networks of Data

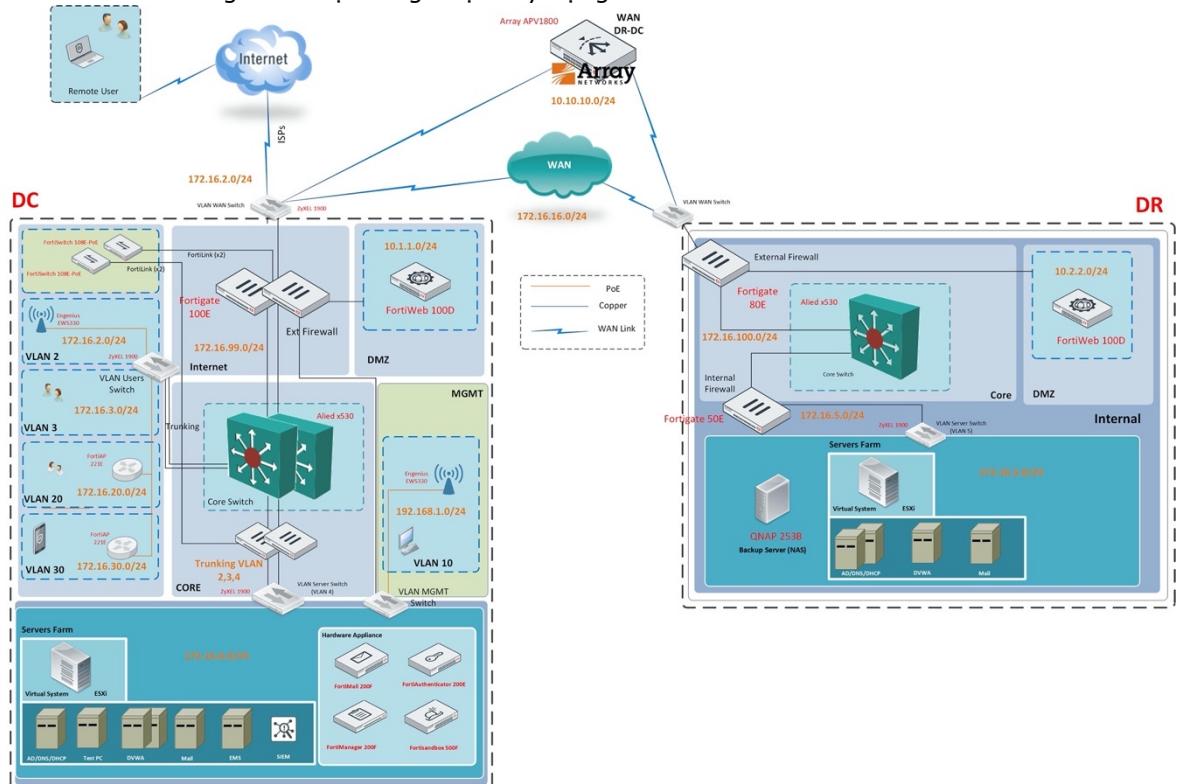
Máy chủ NAS thường có phần mềm mã hóa và là một cách hay để bảo vệ các mạng dữ liệu nhỏ hơn, vì chúng khó tấn công hơn so với máy tính bình thường. Ngoài ra, bất kỳ thứ gì được lưu trữ trên Máy chủ được nối mạng đều được giữ an toàn không chỉ từ các cuộc tấn công bên ngoài mà còn từ việc hỏng các tệp.

Automatic Backing Up of Files

Nhiều máy chủ NAS đi kèm với các cấu hình cho phép sao lưu tự động các dữ liệu. Một thư mục sao chép có thể tồn tại cả trên một máy tính cá nhân, và trên ổ cứng máy chủ, và khi một dữ liệu riêng lẻ trong thư mục được thay đổi trên máy tính, bản sao cũng có thể được thay đổi trên ổ cứng máy chủ. Điều này có thể được thực hiện thông qua cáp ethernet kết nối hoặc trong một số trường hợp không dây.

2 Các thành phần của giải pháp

Mô hình kết nối Logic của hệ thống được xây dựng như sau:



Gồm các thành phần:

2.1 Hạ tầng mạng Access

2.1.1 Mô tả

Phân hệ Access phục vụ cho các kết nối của thiết bị đầu cuối, bao gồm Switch (phục vụ cho kết nối có dây), Wireless Access Point (phục vụ cho kết nối không dây), đây là phân hệ ngoại biên, nhưng đóng vai trò vô cùng quan trọng trong hệ thống, là đầu mối kết nối cho các thành phần thiết bị ngoại vi vào mạng.

Các thiết bị trong phân hệ này sẽ giúp sinh viên hiểu rõ được cách thức kết nối và truy nhập vào hệ thống của tất cả các thiết bị ngoại vi, là kiến thức cơ bản nhất trong các giáo trình mang.

2.1.2 Các thiết bị đầu tư

Thiết bị Access Switch ZyXEL 1900-24HP

Đây là thiết bị Switch 24 Port, có hỗ trợ khả năng cấp nguồn qua giao thức mạng (Power over Ethernet – PoE), phục vụ kết nối cho các thiết bị PC/Laptop, kết nối đến các thiết bị Switch khác và cấp nguồn cho các thiết bị Access Point.

Sinh viên sẽ được tiếp cận với thiết bị này bằng việc thực hành các cấu hình về Vlan, Interface, Trunking, khả năng cấp nguồn PoE, khả năng giám sát...

Các thông số kỹ thuật của thiết bị:

- **Ports** 24 x 10/100/1000 (PoE+) + 2 x Gigabit SFP
- **Power Over Ethernet (PoE)** PoE+
- **PoE Budget** 170W
- **Switching capacity**: 52 Gbps
- **Forwarding performance**: 39 Mbps
- **MAC Address Table** 8K entries
- **Jumbo Frame Support** 9KB
- **Routing Protocol** IGMPv2, IGMP, IGMPv3
- **Remote Management Protocol** SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, SNMP 3
- **Features** Flow control, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, Syslog support, DoS attack prevention, Weighted Round Robin (WRR) queuing, store and forward, IPv6 support, Quality of Service (QoS), LACP support, LLDP support, Port Security, Energy Efficient Ethernet, Management Information Base (MIB), Strict Priority Queuing (SPQ), Class of Service (CoS), tagged VLAN, per port bandwidth control, 525KB packet buffer



Thiết bị FortiSwitch 108E-PoE

Tương tự hệ thống Access Switch của ZyXEL, ngoài nhiệm vụ bảo bảo kết nối cho các thiết bị đầu cuối và cấp nguồn PoE, thiết bị FortiSwitch được đầu tư nhằm hỗ trợ khả năng quản trị bảo mật cho các kết nối này.

FortiSwitch là thiết bị Access được quản lý tập trung bởi Fortigate, từ đó giúp cho việc triển khai các tính năng bảo mật cho hạ tầng mạng Network một cách dễ dàng hơn (L2 Security) như 802.1X, Device management (quản lý các thiết bị kết nối theo hệ điều hành, MAC address...).



Các thông số kỹ thuật:

- **Total Network Interfaces** 8x GE RJ45 and 2x GE SFP
- **RJ-45 Serial Console Port** 1
- **Form Factor** 1 RU Rack Mount
- **Power over Ethernet (PoE)** (802.3af/at)
- **PoE Power Budget** 65 W
- **Mean Time Between Failures** > 10 years
- **Switching Capacity (Duplex)** 20 Gbps
- **Packets Per Second (Duplex)** 30 Mpps
- **MAC Address Storage** 8 K
- **Network Latency** 4μs
- **VLANs Supported** 4 K
- **Link Aggregation Group Size** 8
- **Total Link Aggregation Groups** 8
- **Packet Buffers** 512 KB

- **DRAM** 256 MB DDR3
- **FLASH** 32 MB

Thiết bị Access Point Engenius EWS330AP

Hệ thống Wireless phổ thông, phục vụ các kết nối cơ bản vào phân hệ quản trị, phân hệ LAN User.

Các thông số kỹ thuật:

- Hỗ trợ công nghệ 802.11ac Wave 2.0 để nâng cao băng thông và tốc độ cho các thiết bị không dây (nhanh hơn 30% so với Wave 1)
- Giải pháp Turbo Engine tích hợp cùng với chip xử lý 4-nhân (Quad-core) mạnh mẽ, đảm bảo thực hiện nhiều tác vụ và tăng cường hiệu suất
- Chuẩn 802.11 ac/a/b/g/n (867Mbps @ 5GHz và 400Mbps @ 2.4GHz)
- Hỗ trợ công nghệ MU-MIMO
- Anten MIMO 2 x 2:2
- Công suất phát: 2.4Ghz@26dBm, 5Ghz@26dBm



Thiết bị Access Point FortiAP 221E

Đây là thiết bị Access Point phục vụ cho bảo mật, được quản lý bởi thiết bị Fortigate (External Firewall).

Thiết bị này được đầu tư để mô phỏng cho giải pháp Wireless Controller + Security, giúp Sinh viên hiểu được các cơ chế của hệ thống Wifi được quản lý tập trung, các tính năng phổ biến như khả năng xác thực Portal, các tính năng giám sát thiết bị kết nối...



Các thông số kỹ thuật:

- 802.11ac Wave 2
- Dual Radio 2.4 and 5 GHz
- 4 Internal/External Antennas
- 2x2 MU-MIMO
- Up to 400 + 867 Mbps

2.2 Hạ tầng Mạng Core

2.2.1 Mô tả

Phân hệ mạng Core là thành phần quan trọng của một hệ thống mạng, cho quy mô doanh nghiệp vừa và lớn, đây là phân hệ chuyển mạch xương sống của hệ thống, đóng vai trò xử lý kết nối giữa các phân vùng mạng với nhau, đảm bảo băng thông chuyển mạch tối ưu nhất cho hạ tầng ứng dụng, hạ tầng truy cập của người dùng.

Hệ thống Lab này giúp sinh viên hiểu rõ được các cơ chế chuyển mạch cao cấp hơn, khả năng định tuyến giữa các Vlan, Access Control List, vai trò của LACP, khả năng dự phòng HA...

2.2.2 Các thiết bị đầu tư

Thiết bị Switch Layer 3 x530-28GTXm

Thiết bị đầu tư là Allied Telesis x530-28GTXm, đây là thiết bị Switch Layer 3 cao cấp của thương hiệu đến từ Nhật Bản, với Performance mạnh mẽ và đầy đủ các tính năng phù hợp

cho phân vùng Core của hệ thống. Thiết bị này sẽ kết nối với Firewall mạng biên, Firewall mạng Internal và các thiết bị Access Switch khác.

Thiết bị hỗ trợ sinh viên khả năng tiếp cận dễ dàng thông qua Giao diện Web lẫn bộ lệnh CLI truyền thống (tương tự kiển thức Cisco).

Mô hình được thiết kế HA (Stacking).



Thông số kỹ thuật thiết bị:

- 24 x 10/100/1000 Mbps.
- 4 x SFP+ 10 G (2 if stacked).
- Forwarding rate: 95.2 Million of packets per second (Mpps).
- Switching fabric: 128 Gbps
- Key features: Voice VLAN, VLAN Mirroring (RSPAN), Access Control Lists (ACLs), VLAN ACLs, Storm protection, Loop protection, Support Multicast -IGMP snooping (v1, v2 and v3), Tri-authentication, QoS, Limit bandwidth per port or per traffic, Routing protocols, Static Routing, Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPFv3), Premium Software License AT-FL-X530-01, MSTP, RSTP

2.3 Hạ tầng bảo mật mạng biên

2.3.1 Mô tả

Đây là vùng mạng đóng vai trò Gateway của toàn bộ hệ thống, hỗ trợ khả năng kiểm soát bảo mật cho tất cả các kết nối từ bên trong ra Internet/WAN.

Sinh viên sẽ có được cái nhìn tư cơ bản đến nâng cao với các tính năng của thiết bị như: khả năng định tuyến, các tính năng NAT, khả năng cân bằng tải, phân hoạch Firewall Rule/Policy, các tính năng bảo mật như Antivirus, Web Filtering, Apps Control, IPS... Các tính năng VPN, các tính năng giám sát truy cập của người dùng...

Mô hình được đề xuất đầu tư HA.

2.3.2 Các thiết bị đầu tư

Thiết bị Fortinet Fortigate 100E Bundle

Thiết bị phù hợp cho nhu cầu thực hành Lab, đảm bảo performance để thực hiện các tính năng Firewall mạng biên với tất cả các tính năng từ cơ bản đến nâng cao. Fortinet hiện tại là một trong những nhà cung cấp bảo mật hàng đầu trên thế giới, giúp Sinh viên có cái nhìn thực tế nhất hệ thống bảo mật được sử dụng rộng rãi trong các doanh nghiệp ngày nay.



Thiết bị FG100E Bundle bao gồm đầy đủ các năng lực xử lý phần cứng, tính năng phần mềm, các tiêu chuẩn công nghiệp...hiện đại nhất, là dòng sản phẩm mới của Fortinet, các thông số kỹ thuật:

- **Firewall Throughput (1518 / 512 / 64 byte UDP packets)** 7.4 / 7.4 / 4.4 Gbps
- **Firewall Latency (64 byte UDP packets)** 3μs
- **Firewall Throughput (Packets Per Second)** 6.6 Mpps
- **Concurrent Sessions (TCP)** 2 Million
- **New Sessions/Second (TCP)** 30,000
- **Firewall Policies** 10,000
- **IPsec VPN Throughput (512 byte packets)** 4 Gbps
- **Gateway-to-Gateway IPsec VPN Tunnels** 2,000
- **Client-to-Gateway IPsec VPN Tunnels** 5,000
- **SSL-VPN Throughput** 250 Mbps
- **Concurrent SSL-VPN Users (Recommended Maximum)** 300
- **IPS Throughput (HTTP / Enterprise Mix)** 1.9 Gbps / 500 Mbps
- **SSL Inspection Throughput** 350 Mbps
- **Application Control Throughput** 800 Mbp

2.4 Hạ tầng bảo mật mạng nội bộ

2.4.1 Mô tả

Tương tự phân hệ bảo mật mạng biên, các kết nối từ bên ngoài vào vùng mạng Server ứng dụng của hệ thống cũng cần phải được trang bị bảo mật. Firewall Internal sẽ giúp giải quyết vấn đề này, thiết bị sẽ được triển khai trước vùng mạng của các thiết bị Server, kết nối trực tiếp đến Core Switch, nhằm giám sát bảo mật cho tất cả các luồng dữ liệu ra vào vùng này.

Mô hình sẽ giúp Sinh viên hiểu được nguyên lý hoạt động của bảo mật dữ liệu nội bộ của hệ thống, có cái nhìn chính xác hơn về cách thức vận hành của các tính năng IPS, Antivirus, xác thực, ATP (Sandbox)...

Thiết bị vùng này cũng được đề xuất chạy HA.

2.4.2 Các thiết bị đầu tư

Thiết bị Fortinet Fortigate 80E Bundle

Thiết bị FG80E Bundle phục vụ cho phân hệ này được thiết kế để đảm bảo an toàn cho các Server ứng dụng bên trong ở tầng Network, với năng lực phù hợp để thực hiện các bài Lab thực tế cho Sinh viên.

Thông tin kỹ thuật:

- **GE RJ45/SFP Shared Media Pairs** 2
- **GE RJ45 PoE/+ Ports** 12
- **GE RJ45 DMZ/HA Ports** 2
- **USB Ports** 1
- **Console (RJ45)** 1
- **Firewall Throughput (1518 / 512 / 64 byte UDP packets)** 4 / 4 / 4 Gbps
- **Firewall Latency (64 byte UDP packets)** 3 µs
- **Firewall Throughput (Packets Per Second)** 6 Mpps
- **Concurrent Sessions (TCP)** 1.3 Million
- **New Sessions/Second (TCP)** 30,000
- **Firewall Policies** 5,000
- **IPS Throughput (HTTP / Enterprise Mix)** 1.5 Gbps / 450 Mbps
- **SSL Inspection Throughput** 350 Mbps
- **Application Control Throughput** 800 Mbps
- **NGFW Throughput** 360 Mbps
- **Threat Protection Throughput** 250 Mbps
- **Virtual Domains (Default / Maximum)** 10 / 10



Thiết bị Fortigate 50E Bundle

Thiết bị Fortigate 50E Bundle phục vụ cho phân hệ Internal của site DR, đảm bảo an toàn cho các Server cho hệ thống dự phòng, phù hợp năng lực với việc hỗ trợ các bài Lab cho sinh viên.



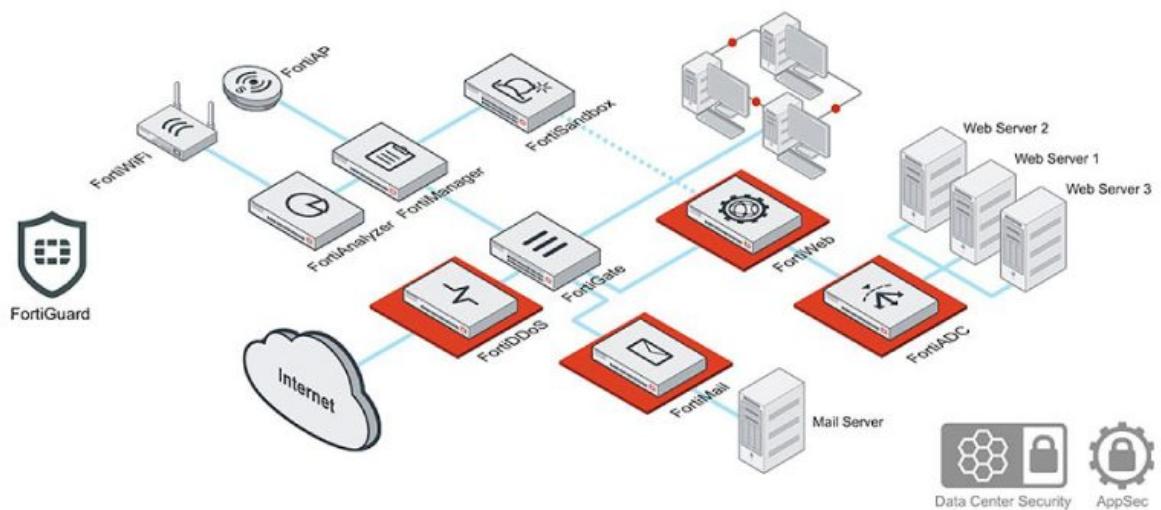
Thông tin kỹ thuật:

- **GE RJ45 Switch Ports:** 5
- **RJ45 WAN Ports:** 2
- **USB Ports** 1
- **Console (RJ45)** 1
- **Firewall Throughput** 2.5Gbps Gbps
- **Firewall Latency (64 byte UDP packets)** 180 µs
- **Concurrent Sessions (TCP)** 1.8 Million
- **New Sessions/Second (TCP)** 21,000
- **Firewall Policies** 5,000
- **IPS Throughput** 350 Mbps
- **NGFW Throughput** 220 Mbps
- **Threat Protection Throughput** 160 Mbps
- **Virtual Domains (Default / Maximum)** 10 / 10

2.5 Hạ tầng Ứng dụng

2.5.1 Mô tả

Phân hệ ứng dụng gồm các thiết bị Server phục vụ cho người dùng như Mail Server, Web Server, Server ứng dụng dành cho doanh nghiệp... Là hệ thống trọng yếu, các Server này cũng cần phải được bảo mật và hỗ trợ bởi các hệ thống khác đi kèm nhằm tối ưu hóa hiệu năng và đảm bảo an toàn, phòng chống các nguy cơ xâm nhập, gián đoạn hệ thống.



Mục đích của việc đầu tư tại phân hệ này nhằm giúp sinh viên có cái nhìn sâu hơn về các hệ thống bảo mật ứng dụng, Firewall chỉ đóng vai trò bảo vệ cho hệ thống mạng, các hệ thống bảo mật ứng dụng sẽ cần những hệ thống bảo mật cao cấp hơn mới có thể đáp ứng được cả về năng lực xử lý lẫn các tính năng.

Tại đây, chúng ta sẽ có thiết bị Email Gateway Security bảo mật cho hệ thống Mail Server, Web Application Firewall phục vụ bảo mật cho hệ thống Web Server, và hệ thống Application Delivery Controller phục vụ cho việc cân bằng tải cho các Server ứng dụng.

Các thiết bị này sẽ được triển khai tại vùng DMZ

2.5.2 Các thiết bị đầu tư

Thiết bị Fortinet FortiMail 200F Bundle

Thiết bị sẽ đóng vai trò là Mail Gateway của hệ thống, toàn bộ lưu lượng Email ra vào Mail Server sẽ được kiểm soát và thực thi các tính năng bảo mật như AntiSpam, AntiVirus, giám sát việc gửi nhận Mail, Archive Mail, FortiMail 200F có năng lực vừa đủ để đáp ứng việc thực hành Lab toàn bộ các tính năng này trên hệ thống Mail già lập, các thông số kỹ thuật của thiết bị:



- **10/100/1000 Interfaces (Copper, RJ-45)** 4
- **Storage** 1TB
- **Form Factor** 1U Rack
- **Protected Email Domains:** 20
- **Server Mode Mailboxes** 150
- **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** 50/60
- **Performance (Messages/Hour) [Without queuing based on 100 KB message size]**
- **Email Routing** 50 K
- **FortiGuard Antispam** 40K
- **FortiGuard Antispam + Antivirus** 30 K

Thiết bị Fortinet FortiWeb 100D Bundle

Web Application Firewall đóng vai trò quan trọng trong việc bảo vệ cho hệ thống Web Server, điều mà bản thân các thiết bị Network Firewall không làm được.

FortiWeb 100D có Performance vừa đủ để triển khai các tính năng bảo mật Web đáp ứng được các nhu cầu giảng dạy và giúp sinh viên có được cái nhìn thực tế về các tính năng hiện đại như SQL Injection, XSS, AntiDefacement, DoS Protection...với hệ thống Web giả lập.



Thống số kỹ thuật:

- **10/100/1000 Interfaces (RJ-45 ports)** 4
- **SSL/TLS Processing** Software
- **USB Interfaces** 2
- **Storage** 16 GB
- **Form Factor** Desktop
- **Power Supply** Single
- **Throughput** 25 Mbps
- **Latency** Sub-ms

Thiết bị Array Network APV1800 AppVelocity

Với các hệ thống Server hiện đại ngày nay, để phục vụ cho một số lượng lớn các truy cập đồng thời từ người dùng, phải có sự hỗ trợ của các hệ thống ADC (hay còn gọi là hệ thống cân bằng tải ứng dụng), nhằm mục đích tăng khả năng phục vụ cùng với việc đảm bảo tính dự phòng, tính liên tục của toàn bộ các ứng dụng quan trọng cho cơ quan/doanh nghiệp.

Thiết bị APV1800 với thiết kế cho quy mô nhỏ nhất, đáp ứng được nhu cầu thực hành Lab của Sinh viên cho các hệ thống ứng dụng giả lập, đem lại cái nhìn trực quan nhất về cách thức hoạt động của các bộ tính năng cân bằng tải, thuật toán sử dụng như Round Robin, Weight, Less Session, Respond time... ,các tính năng Healthchecking, khả năng SSL

Offloading, ... là sự ứng dụng các kiến thức đã học được trong chuyên ngành Mạng máy tính từ Networking cho đến Application.



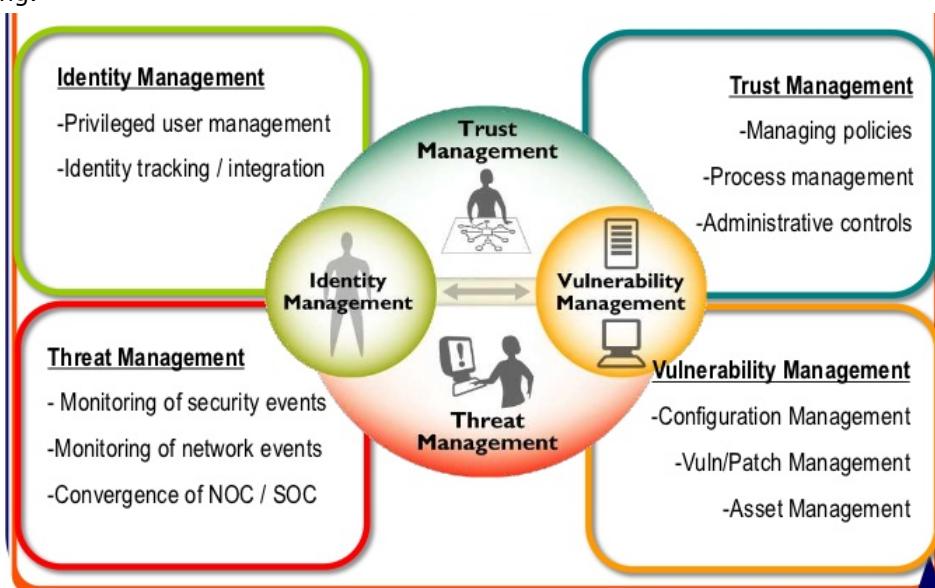
Thông số kỹ thuật của thiết bị:

- **Max. L4 Throughput** 7 Gbps
- **Max. SSL Throughput** 7 Gbps
- **Max. SSL TPS (RSA 2K)** 20K
- **Max. ECC TPS (ECDSA P256)** 14K
- **L2, L4 & L7 SLB** Yes
- **L7 Policy Engine** Yes
- **ePolicy Scripting** Yes
- **eRoute Routing** Yes
- **Transparent Proxy** Yes
- **SSL (HW)** Yes
- **Compression (SW)** Yes
- **RAM Caching** Yes

2.6 Hạ tầng Quản lý

2.6.1 Mô tả

Hạ tầng quản lý đóng vai trò quan trọng trong mô hình doanh nghiệp hiện đại, là công cụ để đội ngũ nhân viên IT triển khai, vận hành, quản trị, khắc phục sự cố cho toàn bộ hệ thống.



Với sự phát triển nhanh chóng của các công nghệ hiện đại, các hệ thống quản lý vận hành CNTT ngày càng đáp ứng được các nhu cầu chi tiết của người quản trị, từ thao tác cài đặt triển khai, giám sát cho đến báo cáo, khắc phục sự cố...đều được phục vụ một cách tốt nhất. Bên cạnh đó, việc tiếp cận để làm chủ được các hệ thống này cũng đòi hỏi người kỹ

sư cũng phải có được các kiến thức nền tảng, các kinh nghiệm nhất định liên quan, do đó, việc giúp sinh viên tiếp cận sớm với các hệ thống này cũng là một sự cần thiết để các em có được cái nhìn thực tế sau khi ra trường, cơ hội tiếp cận sớm với các giải pháp hiện đại này cũng là một lợi thế khi các em ứng tuyển vào các doanh nghiệp lớn.

Các giải pháp quản lý tập trung mà Tech Horizon muốn xây dựng cho nhà trường bao gồm:

- Hệ thống quản lý và lưu trữ Log tập trung cho các thiết bị Fortinet,
- Giải pháp xác thực Radius
- Hệ thống quản lý bảo mật tập trung cho Endpoint
- Hệ thống bảo mật ATP Sandbox
- Giải pháp quản trị sự kiện bảo mật (SIEM)

2.6.2 Các thiết bị đầu tư

Thiết bị FortiManager 200F

Đây là giải pháp quản lý và lưu trữ Log tập trung cho tất cả các thiết bị Fortigate trong hệ thống, hỗ trợ khả năng cấu hình, giám sát và lưu trữ tất cả các Log từ Fortigate, giúp nâng cao khả năng quản trị.

Ngoài Fortigate, thiết bị còn tương thích với các sản phẩm khác như FortiWeb, FortiClient, FortiAP..., phục vụ các tính năng như triển khai đồng bộ, giám sát License, cấu hình đồng bộ, gửi nhận thông báo trên toàn hệ thống cho người quản trị thông qua Email, SMS, hỗ trợ xuất Report theo yêu cầu, thời gian lưu trữ Log lâu dài...



Thông số kỹ thuật của thiết bị FortiManager 200F:

- | | |
|--|-----------------|
| • GB/Day of Logs | 100 |
| • Analytic Sustained Rate (logs/sec) | 3,000 |
| • Collector Sustained Rate (logs/sec) | 4,500 |
| • Devices/VDOMs (Maximum) | 150 |
| • Max Number of Days Analytics | 40 |
| • Form Factor | 1 RU Rackmount |
| • Total Interfaces | 2xRJ45 GE |
| • Storage Capacity | 4 TB (1 x 4 TB) |

Thiết bị FortiAuthenticator 200E

Trong các hệ thống doanh nghiệp hiện đại, xác thực là thành phần quan trọng để bảo mật cho toàn bộ các truy cập.

Các hệ thống quan trọng như Ứng dụng, hệ thống Portal truy cập Wireless, hệ thống xác thực VPN, cần 1 thiết bị hỗ trợ LDAP/RADIUS được xây dựng chuyên biệt để phục vụ, FortiAuthenticator ngoài các tính năng và dịch vụ cơ bản để chạy các tính năng này, còn hỗ trợ thêm các thành phần như: xác thực 2 bước (Two-Factor), quản lý các chính sách Password, hệ thống cảnh báo, cho phép người dùng thay đổi Password...

Các tính năng này sẽ giúp sinh viên tiếp cận được các công nghệ xác thực hiện đại đang được ứng dụng rộng rãi, là nền tảng của hệ thống bảo mật.



Thông số kỹ thuật của thiết bị:

- **10/100/1000 Interfaces (Copper, RJ-45)** 4
- **Local Storage** 1 x 1 TB Hard Disk Drive
- **Power Supply** Single 480W Auto Ranging (100V–240V)
- **Total Users (Local + Remote)** 500
- **FortiTokens** 500
- **RADIUS Clients (NAS Devices)** 50
- **User Groups** 50
- **CA Certificates** 10
- **User Certificates** 2,500

Hệ thống quản lý bảo mật EndPoint FortiClient EMS

Fortinet hỗ trợ giải pháp FortiClient cho thiết bị đầu cuối của người dùng, tính năng này được tích hợp tương tự như một Personal Firewall trên mỗi thiết bị PC/Laptop/Mobile.

Các tính năng hỗ trợ chính của FortiClient tương tự như trên một thiết bị Fortigate :

Antivirus	Application Firewall	Web Filter	Vulnerability Scanning
Real-time Host Protection	Network Activity Detection	Cloud based URL rating	Up-to-date Applications
Updates Every Hour	Application Categories	Safe Search Option Exclusion List	Automated Patching
Scheduled Scanning	Individual Application Granularity		Scheduled Scanning

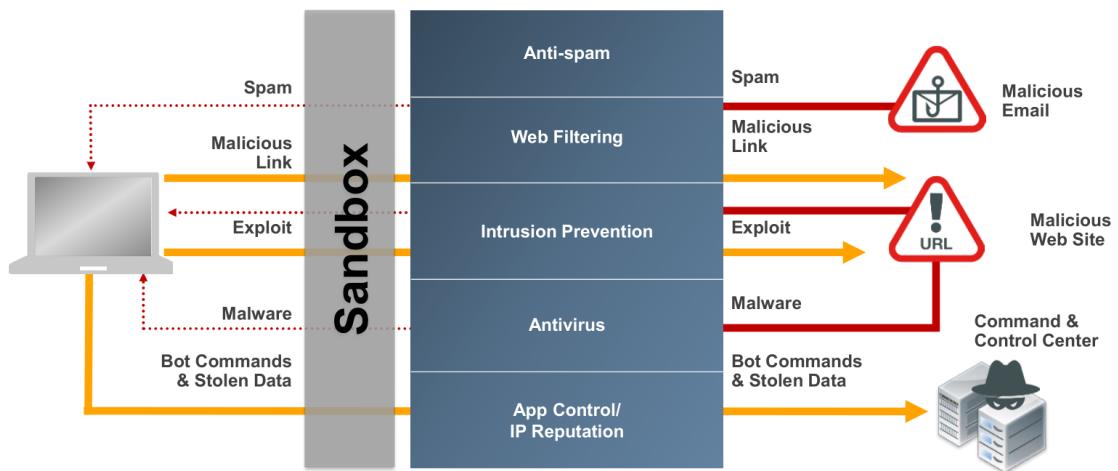
Đặc biệt, trong xu hướng trang bị các hệ thống ATP, Forticlient cũng hỗ trợ người dùng đầu cuối khả năng dò quét các dạng tấn công ZeroDay/APT một cách hiệu quả nhờ kết hợp với giải pháp FortiSandbox từ Fortinet.

FortiClient EMS là nền tảng quản lý tập trung của toàn bộ các Endpoint này, giúp việc giám sát bảo mật cho toàn bộ các Endpoint được thực hiện một cách đơn giản nhất.

Thiết bị FortiSandbox 500F Bundle

FortiSandbox hướng tới việc tái tạo hành vi người dùng thực trên hệ thống để thực thi và tăng tốc các mã độc hại để phát hiện ra các mã độc hại này. Để đánh giá mã độc hại, sandbox sẽ chạy với nhiều tiến trình code trên nhiều hệ điều hành và công nghệ khác

nhau.



FortiSandbox là công cụ phát hiện hoạt động các tốt nhất kết hợp với khả năng thực thi và phòng chống của tường lửa, Mail Gateway hay Endpoint tạo thành hệ thống phòng chống các hiểm họa thế hệ mới.. Thiết bị chứng minh 99% phát hiện vi phạm trong bài test các vi phạm trong hệ thống của NSS Lab.

Với các thiết bị Fortinet đã được đầu tư để xây dựng mô hình Lab bảo mật, FortiSandbox là thiết bị không thể thiếu để giúp sinh viên có thể tiếp cận đến 1 trong những xu thế bảo mật hiện đại nhất ngày nay – Advance Threat Protection.



Thông số kỹ thuật của thiết bị:

- **Form Factor** 1 RU
- **Total Network Interfaces** 4x GE RJ45 ports
- **Storage Capacity** 1x 1 TB
- **Power Supplies** 1x PSU
- **Number of VMs** 6
- **Sandbox Pre-Filter Throughput (Files/Hour)** 4,500
- **VM Sandboxing Throughput (Files/Hour)** 120
- **Real-world Effective Throughput (Files/Hour)** 600
- **Sniffer Throughput** 500 Mbps

Hệ thống SIEM

FortiSIEM là một giải pháp Next-Gen SIEM, tích hợp tính năng của một giải pháp Security Incident and Event Management (SIEM) với một giải pháp Performance & Availability

monitoring (PAM), giúp thu thập và phân tích từ rất nhiều nguồn thông tin khác nhau, trong đó có Log, performance metrics, SNMP Traps, security alerts và những thay đổi về cấu hình (configuration change). Nói một cách khác, FortiSIEM có thể kết hợp dữ liệu thường được thu thập riêng rẽ giữa một SOC (SIEM) và một NOC (PAM) để tạo thành một bức tranh tổng thể về các mối đe dọa có thể tồn tại trong hệ thống.

- FortiSIEM được cung cấp dưới dạng Virtual Appliance, hỗ trợ triển khai on-premise và rất nhiều các nền tảng private và public cloud bao gồm: VMware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure.
- Một số hãng SIEM tồn tại nhiều giao diện quản trị GUI riêng biệt để quản lý platform của họ, ví dụ như một cho Log Management, một database khác để Filter dữ liệu và cuối cùng một database khác để thực hiện Analytics. Với FortiSIEM, tất cả các tính năng được quản trị thông qua một giao diện quản trị duy nhất.
- FortiSIEM hỗ trợ cơ chế license linh hoạt, với việc mua license theo số lượng thiết bị và số lượng Event per second (EPS), dễ dàng khi mở rộng.

Hệ thống này sẽ giúp Sinh viên tiếp cận được với công nghệ quản trị hệ thống hiện đại nhất hiện nay, với các thành phần được xây dựng dựa trên các mô hình thực tế cho doanh nghiệp.

2.7 DR-DC

Được đầu tư theo mô hình DR-DC, hệ thống với toàn bộ phân vùng Ứng dụng (không bao gồm phân vùng Access) sẽ được giả lập dự phòng (DR) ở 1 Site hoạt động song song với toàn bộ Site chính (DC).

Hệ thống dự phòng sẽ bao gồm:

- Firewall External FG80E Bundle
- Firewall Internal FG50E Bundle
- Web Application Firewall FortiWeb 100D
- Coreswitch x530-28GTXm
- Access Switch ZyXEL GS1900-24HP
- QNAP TS-253B-4G phục vụ lưu trữ NAS Backup

Hệ thống sẽ dự phòng theo cơ chế chuyển đổi truy cập giữa các Site, khi một trong các thành phần của phân hệ Ứng dụng tại Site DC gặp sự cố, thì toàn bộ các truy cập từ bên ngoài vào hệ thống sẽ được chuyển đổi sang Site dự phòng, theo các tính năng phân giải DNS giả lập ở kết nối WAN bên ngoài.

Các cấu hình giữa 2 Site phải tương đồng, từ thành phần Networking cho đến Bảo mật, và quan trọng nhất là Data trên hệ thống Server.

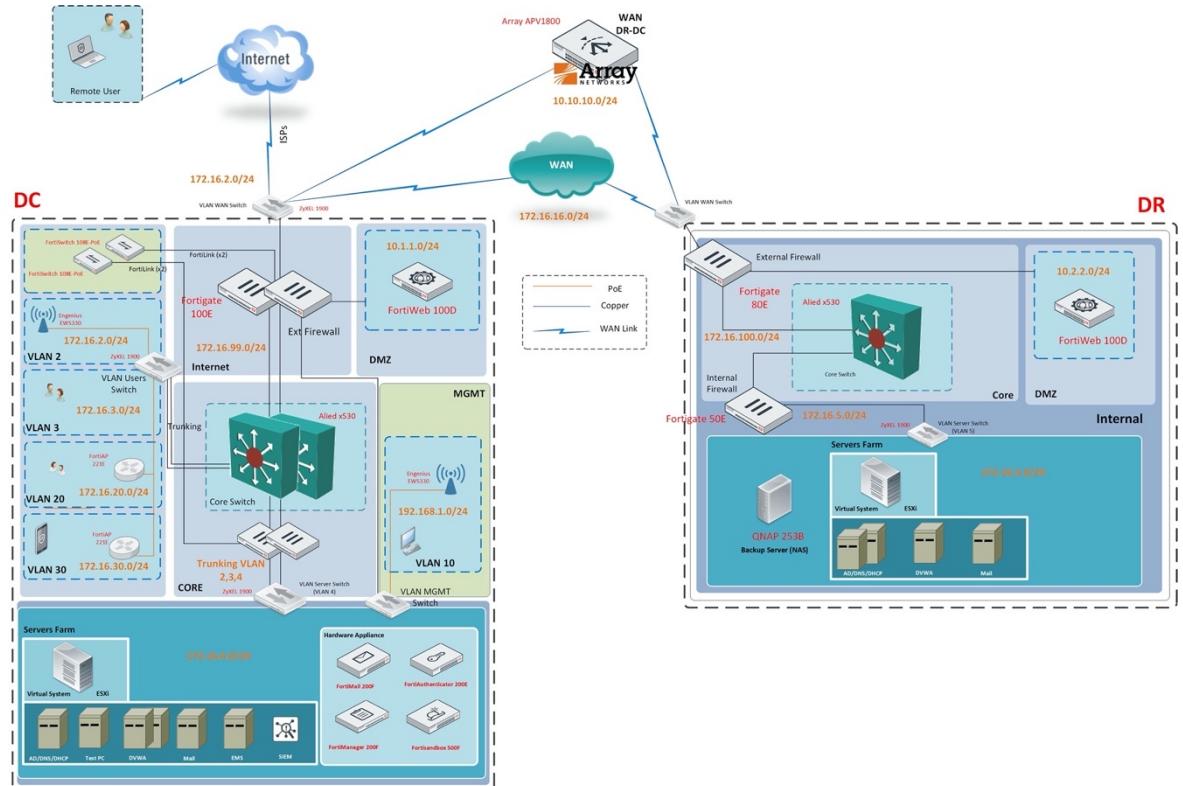
Thiết bị QNAP cho mục này, nhằm hỗ trợ thực hiện các tính năng Backup dữ liệu tự động cẩn thiết từ Site chính DC, đảm bảo dữ liệu luôn được khôi phục kịp thời trong mọi tình huống xấu nhất.Thông tin thiết bị QNAP:



- **CPU Architecture** 64-bit x86
- **Graphic Processors** Intel® HD Graphics 500
- **Floating Point Unit**
- **Encryption Engine** (AES-NI)
- **Hardware-accelerated Transcoding**
- **System Memory** 4 GB SO-DIMM DDR3L (2 x 2 GB)
- **Maximum Memory** 8 GB (2 x 4GB)
- **Memory Slot** 2 x SO-DIMM DDR3L
- **Drive Bay** 2 x 3.5-inch SATA 6Gb/s, 3Gb/s
- **Drive Compatibility** 3.5-inch SATA hard disk drives
- **Gigabit Ethernet Port (RJ45)** 2
- **Dung lượng lưu trữ đầu tư:** 2 HDD 14TB SATA.

3 Các nội dung thực hành Lab

Mục đích của dự án này là dựa trên toàn bộ hệ thống thiết bị đầu tư để xây dựng các bài Lab thực tế để giúp sinh viên tiếp cận trực tiếp với các công nghệ đang được sử dụng rộng rãi trong môi trường doanh nghiệp.



Nội dung các phần thực hành Lab bao gồm:

3.1 Hệ thống Network

3.1.1 Access Network

Thực hành các tính năng Layer 2 của trên các thiết bị Switch Access và Access Point trong mô hình của hệ thống, bao gồm:

Mạng có dây

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị
- Thực hành về phân hoạch IP
- Thực hành chia Vlan theo từng cum Interface trên các thiết bị Switch
- Thực hành Trunking giữa các thiết bị Switch

Mạng không dây

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị
- Thực hành cấu hình giao diện quản trị, các tính năng cơ bản (NTP, Firmware,...)
- Thực hành các khả năng xác thực trên từng SSID (WPA2/Portal)
- Thực hành các tính năng Roaming
- Thực hành các tính năng MESH

3.1.2 Core Network

Thực hành các tính năng Layer 3 trên mô hình của hệ thống, bao gồm:

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị

- Thực hành các tính năng LACP (802.3ad)
- Thực hành tính năng Routing giữa các VLAN
- Thực hành các tính năng Routing
- Thực hành tính năng DHCP

3.2 Hệ thống bảo mật

3.2.1 Bảo mật mạng biên

Thực hành các tính năng bảo mật cho người dùng kết nối Internet từ các thiết bị ngoại vi, trực tiếp trên thiết bị External Firewall trong mô hình của hệ thống, nội dung các bài Lab:

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị
- Thực hành các tính năng Network cơ bản: IP, NAT, Port Forwarding
- Thực hành kiểm soát hệ thống theo các dịch vụ (Layer 4 Port)
- Thực hành kiểm soát hệ thống theo người dùng (User)
- Thực hành kiểm soát hệ thống theo thiết bị đầu cuối (Device Management, kết hợp với Access Point, Switch)
- Thực hành các tính năng kiểm soát ứng dụng (Facebook, Youtube...)
- Thực hành các tính năng kiểm soát Web
- Thực hành các tính năng kiểm soát băng thông truy cập
- Thực hành các tính năng giám sát Log và Traffic

3.2.2 Bảo mật mạng nội bộ

Thực hành các tính năng bảo mật trên thiết bị Firewall Internal, đảm bảo an toàn cho hệ thống các Server bên trong, bao gồm các tính năng:

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị
- Thực hành khả năng phòng chống tấn công với IPS (sử dụng các công cụ tấn công để thử nghiệm)
- Thực hành khả năng phòng chống Virus (dùng các mẫu thử Virus)
- Thực hành khả năng phòng chống các dạng Advance Malware (kết hợp với hệ thống Sandbox)

3.2.3 Bảo mật Mail

Thực hành các tính năng bảo mật cho hệ thống Email Server, trực tiếp trên thiết bị Mail Gateway, bao gồm:

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị
- Thực hành khả năng phòng chống Spam (với các Email Spam thử nghiệm từ bên ngoài, hoặc tự tạo)
- Thực hành khả năng phòng chống Virus cho hệ thống Mail (các Email đính kèm có chứa Virus thử nghiệm)
- Thực hành khả năng kiểm soát Email ra vào hệ thống (theo người gửi/nhận, theo IP, theo nội dung, theo từ khóa Subject...)
- Thực hành khả năng giám sát traffic Mail

3.2.4 Bảo mật Web

Thực hành các tính năng bảo mật cho hệ thống ứng dụng Web, trực tiếp trên thiết bị Web Application Firewall theo mô hình đã thiết kế, gồm:

- Thực hành tìm hiểu các tính năng trên giao diện quản lý của thiết bị
- Thực hành kiểm soát và phòng chống SQL Injection/XSS cho Web Site
- Thực hành kiểm soát và phòng chống DDOS cho Web Site
- Thực hành kiểm soát và phòng chống Virus cho Web Server

- Thực hành khả năng Scan lỗ hổng Web
- Thực hành khả năng giám sát traffic Web

3.2.5 Cân bằng tải Ứng dụng

Tiếp xúc trực tiếp với hệ thống cân bằng tải ứng dụng trên thiết bị ADC, các tính năng thực hành bao gồm:

- Thực hành tìm hiểu các tính năng trên giao diện quản trị của thiết bị
- Thực hành các tính năng cân bằng tải cho Server ứng dụng theo thuật toán
- Thực hành cân bằng tải kết nối DR-DC

3.2.6 Bảo mật Endpoint

Thực hành trên thiết bị đầu cuối của người dùng, với phần mềm Client Security, các tính năng:

- Thực hành tìm hiểu các thành phần trên giao diện quản lý của hệ thống
- Thực hành khả năng giám sát Client tập trung từ giao diện quản lý
- Thực hành khả năng Quét Virus tập trung
- Thực hành khả năng triển khai tính năng giám sát ứng dụng
- Thực hành khả năng giám sát các thông tin trên máy trạm của người dùng(OS, phần mềm đã được cài đặt, Username...)

3.2.7 Hệ thống xác thực tập trung

Thực hành kết nối các thiết bị bảo mật khác vào hệ thống xác thực, theo mô hình thiết kế, bao gồm các thành phần:

- Tìm hiểu các thành phần trên thiết bị, giao diện quản trị
- Thực hành kết nối thiết bị với các hệ thống khác: External Firewall, Internal Firewall, Wireless...
- Thực hành các tính năng LDAP, phân quyền
- Thực hành các tính năng xác thực 2 bước
- Thực hành khả năng giám sát xác thực

3.2.8 Hệ thống phòng chống APT

Thực hành các tính năng trên thiết bị Sandbox khi tích hợp với các thiết bị bảo mật khác trong hệ thống.

- Tìm hiểu các thành phần trong giao diện quản trị thiết bị
- Thực hành kết nối thiết bị tới các hệ thống bảo mật khác: Fortigate, FortiWeb, FortiMail...
- Thực hành khả năng kiểm soát APT của thiết bị
- Thực hành khả năng giám sát, Report

3.3 Hệ thống quản lý

3.3.1 Hệ thống quản lý các thiết bị Firewall

Hỗ trợ sinh viên có cái nhìn tổng quan về việc quản lý tập trung các thiết bị Firewall trong toàn bộ hệ thống, gồm các bài Lab:

- Thực hành tìm hiểu tổng quan các thành phần cấu hình trên thiết bị
- Thực hành add các thiết bị Firewall được quản lý vào hệ thống
- Thực hành đồng bộ các cấu hình từ Firewall được quản lý vào hệ thống
- Thực hành cấu hình các tính năng cơ bản tập trung từ thiết bị quản lý cho toàn bộ hệ thống (Network IP, Object, Policy)
- Thực hành các tính năng lưu trữ Log tập trung
- Thực hành các tính năng Report tập trung
- Thực hành các tính năng cảnh báo tập trung

3.3.2 Hệ thống quản lý SIEM

Xây dựng các bài Lab tổng thể cho hệ thống SIEM, bao gồm:

- Thực hành tìm hiểu tổng quan các thành phần cấu hình trên thiết bị
- Thực hành giám sát các thiết bị Network được quản lý trên SIEM: Switch Acess, Core Switch, Wireless...
- Thực hành khả năng thực thi các chính sách truy cập, các chính sách bảo mật
- Thực hành khả năng kiểm tra Log của các thiết bị
- Thực hành các tính năng cảnh báo

3.3.3 Hệ thống lưu trữ NAS

Các bài Lab phục vụ cho mô hình Lưu trữ, Backup dữ liệu, bao gồm:

- Thực hành tìm hiểu tổng quan các thành phần cấu hình trên thiết bị
- Thực hành các tính năng về RAID
- Thực hành các tính năng phân quyền
- Thực hành các tính năng Backup

3.4 DR-DC

Mô hình DR-DC giúp sinh viên có cái nhìn trực quan nhất về khả năng chạy dự phòng đối với các doanh nghiệp quy mô lớn, đòi hỏi sinh viên phải có các kiến thức nền tảng về Network, System... để tiếp thu được các nguyên tắc dự phòng ở mỗi Site cũng như ở nhiều Site.

3.4.1 Khả năng đồng bộ

Các bài Lab thực hành:

- Tìm hiểu tổng quan về HA của hệ thống
- Thực hành các tính năng đồng bộ Data giữa các Site, giữa các thiết bị

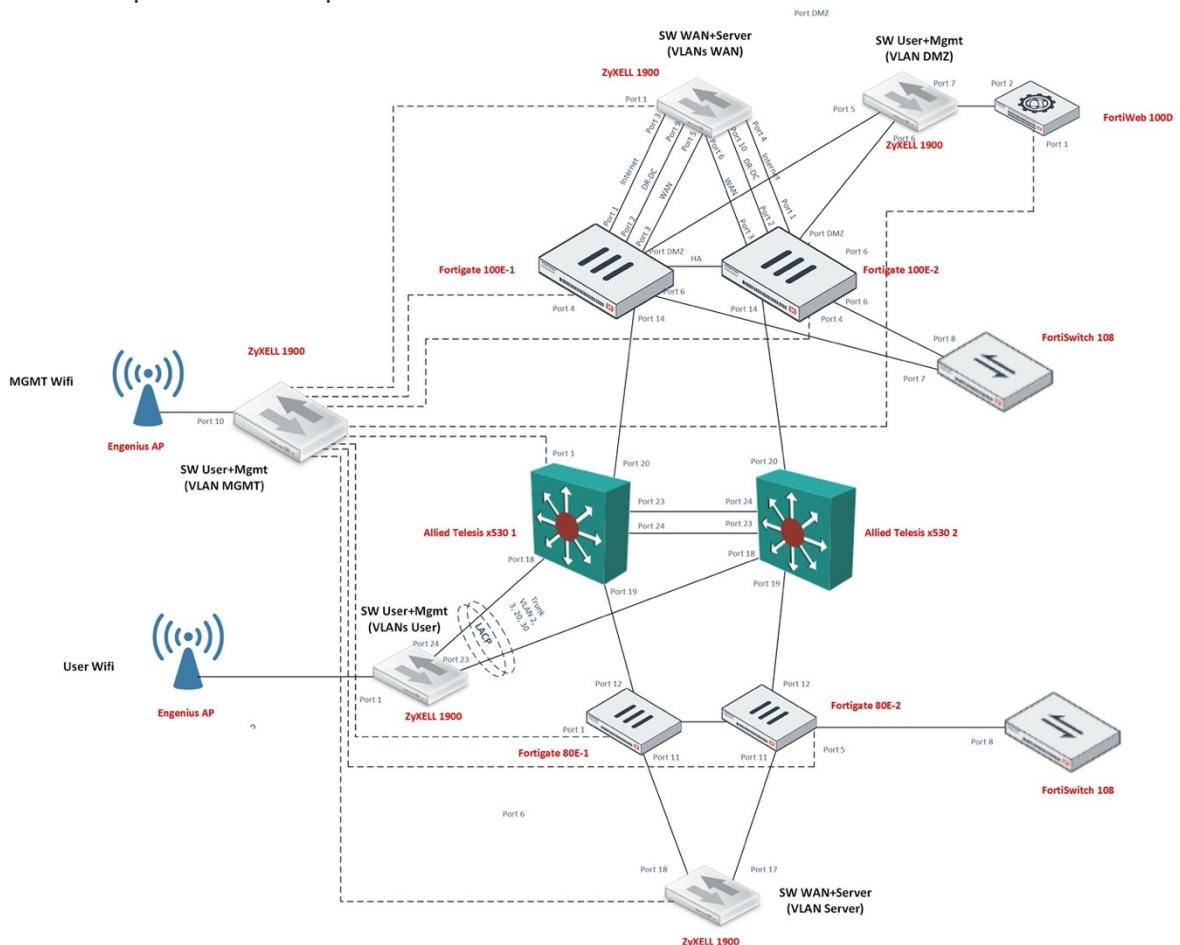
3.4.2 Khả năng dự phòng

- Các bài Lab thực hành về khả năng chạy dự phòng giữa các Site (DR-DC)

4 Mô hình kết nối Vật lý

4.1 Các thiết bị trung tâm

Các thiết bị chính kết nối tại Site DC.



Mô hình này gồm các kết nối vật lý giữa các thiết bị.

Toàn bộ các thiết bị này sẽ được quản trị bởi một lớp mạng riêng (192.168.1.0/24). Để dự phòng các vấn đề lỗi kết nối. Mạng này sẽ kết nối trực tiếp ra Firewall External (FG100E).

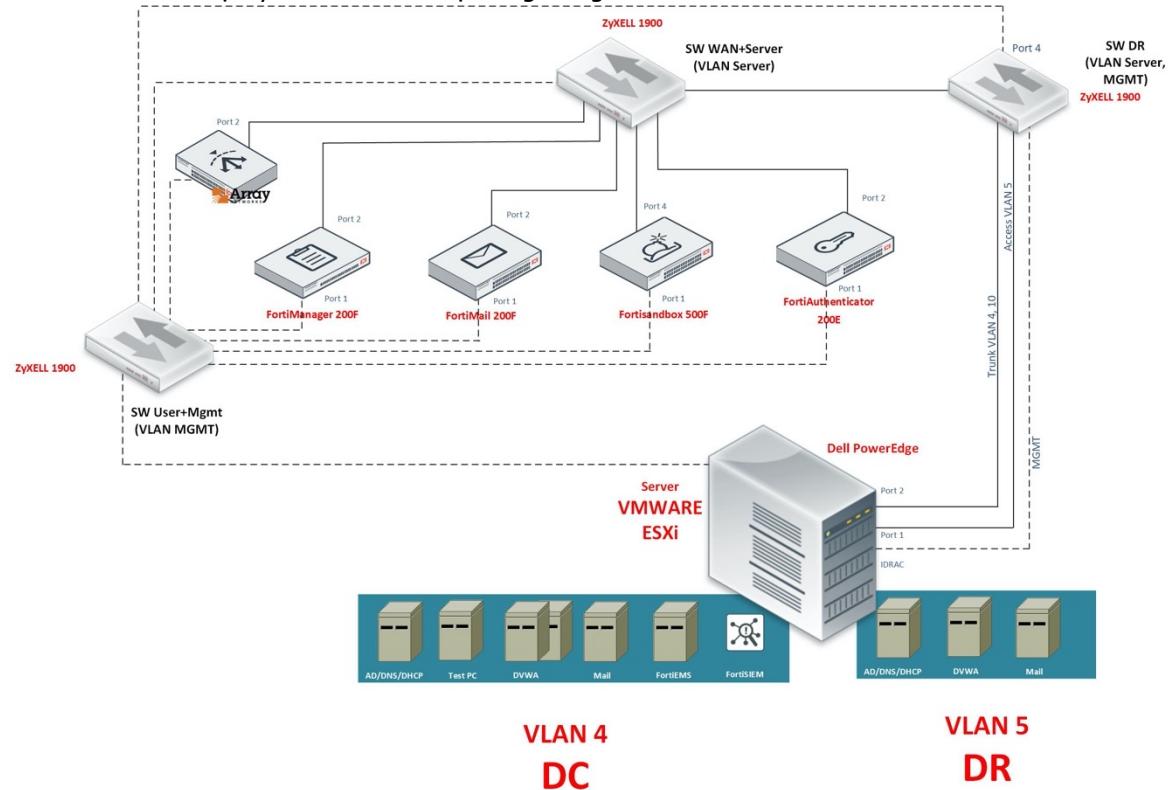
Thiết bị Switch Access 1900 dành cho vùng MGMT sẽ được sử dụng để kết nối quản trị đến toàn bộ các thiết bị.

Phân hệ Core chạy dự phòng các thiết bị Allied Telesis và Fortigate 100E+80E, hỗ trợ dự phòng cho hệ thống.

Lưu ý: hệ thống gồm 3 thiết bị Switch ZyXEL 1900 hỗ trợ chia VLAN để phục vụ cho kết nối giữa các thiết bị. Chi tiết về Port kết nối và VLAN của 3 thiết bị này, tham khảo tại **mục 6.2**.

4.2 Các thiết bị trong vùng Server

Mô hình kết nối vật lý cho các thiết bị trong vùng Server

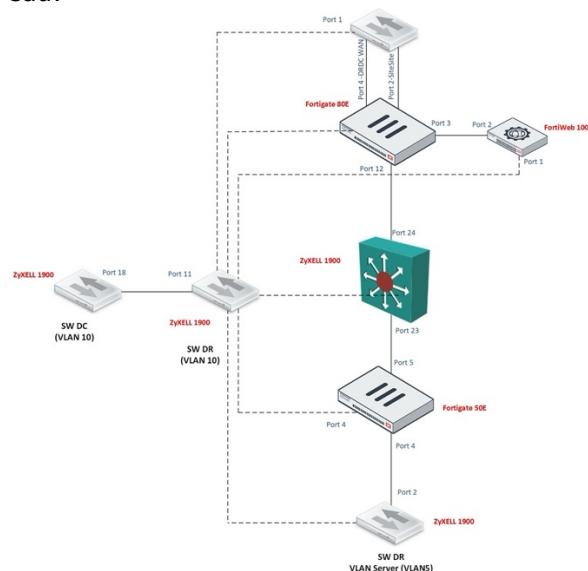


Vùng Server gồm các thiết bị Fortinet, Array Network và Server Dell PowerEdge phục vụ ảo hoá. Bên trong Server này gồm nhiều các Server khác phục vụ ứng dụng của hệ thống. Server này sẽ được chia làm 2 VLAN: VLAN 4 phục vụ cho Server của vùng DR, VLAN 5 phục vụ cho Server của vùng DR (tận dụng).

Mô hình này cũng sử dụng đến 3 thiết bị Switch ZyXEL 1900, với các phân hoạch port như mô tả trong **mục 6.2**.

4.3 Các thiết bị chính tại Site DR

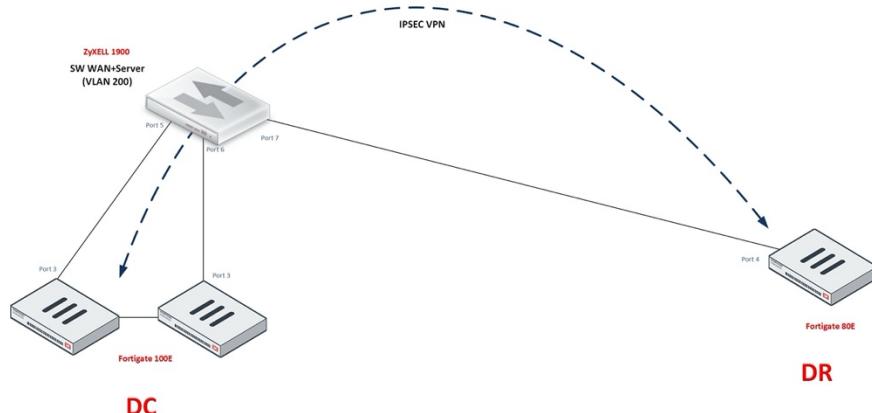
Mô hình kết nối tại Site DR sẽ không gồm các thiết bị HA, mô hình sẽ đơn giản hơn như sau:



4.4 Các thiết bị khác

4.4.1 Vùng kết nối WAN đồng bộ Site to Site

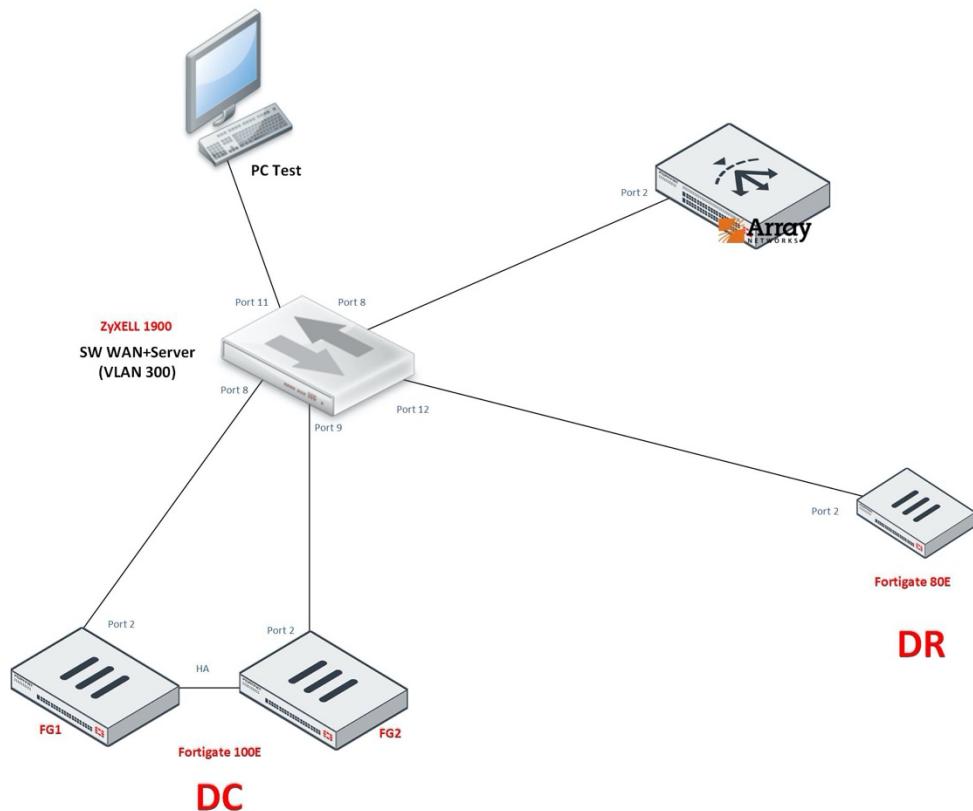
Đây là mô hình kết nối giữa 2 Site với nhau phục vụ việc đồng bộ giữa 2 Site, qua giao thức VPN IPSEC.



Các thiết bị sẽ tận dụng việc chia VLAN trên Access Switch dành cho vùng WAN để kết nối (VLAN 200).

4.4.2 Vùng kết nối WAN DR-DC

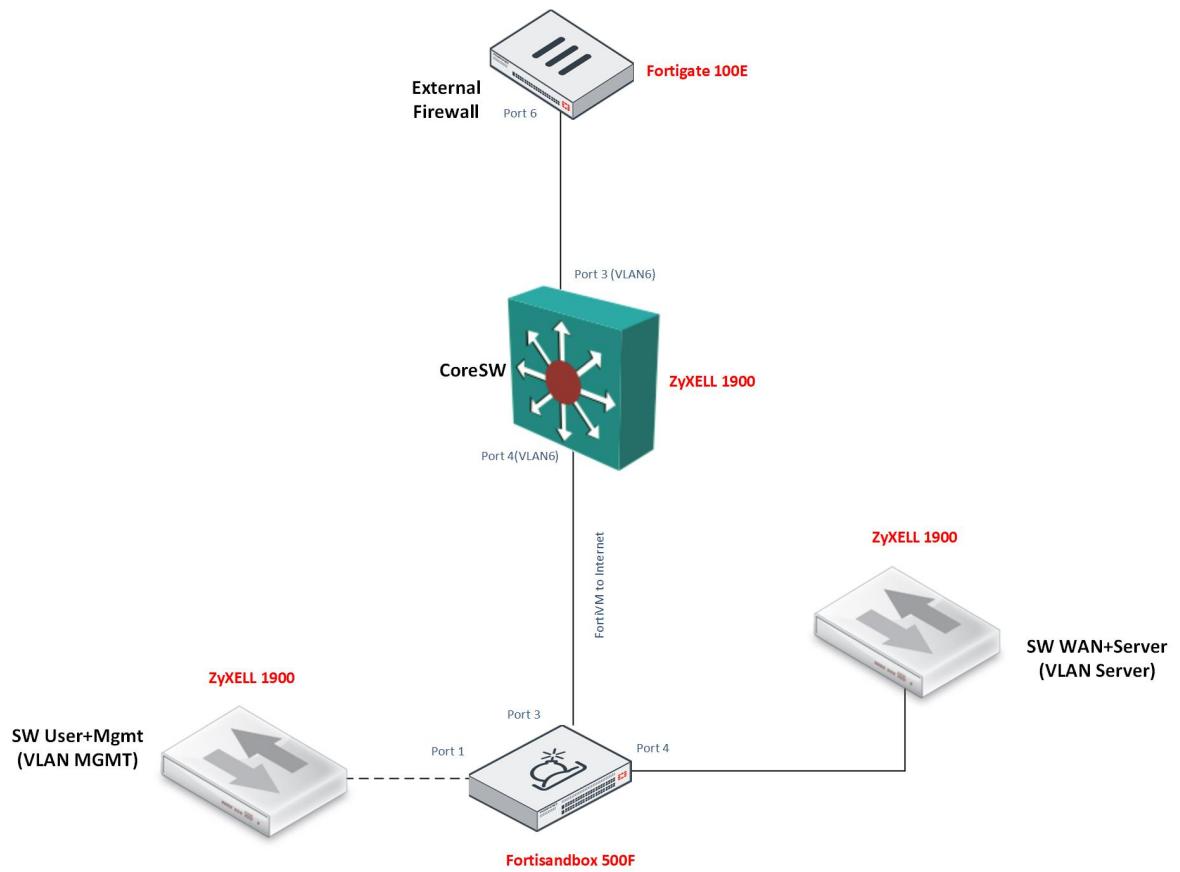
Mô hình này thể hiện kết nối DR-DC giữa 2 thiết bị, sở dĩ mô hình này được tách riêng để phục vụ cho việc Test các tính năng DR-DC, người dùng sẽ kết nối trực tiếp vào vùng này để Test.



Tận dụng khả năng VLAN của Switch dành cho vùng WAN (VLAN 300)

4.4.3 Thiết bị FortiSandbox

Do kiến trúc đặc biệt, thiết bị FortiSandbox cần 1 đường kết nối riêng, tách biệt với hệ thống mạng để trực tiếp ra Internet dành cho các máy ảo VM trên đó. Nên mô hình cho thiết bị này được quy hoạch trong hệ thống như sau:



5 Quy hoạch hệ thống

5.1 Quy hoạch IP và Kết nối

Site DC: được quy hoạch IP và đấu nối như sau:

	Thiết Bị	VLAN	IP	Port	Mô Tả
Vùng Internet					
1	FortiGate 100E		10.1.1.254/24	dmz	Kết nối với FortiWeb qua Switch DMZ
			10.20.0.1/24	Port 1	WAN Internet
			10.10.10.11/24	Port 2	Mạng DR-DC WAN giả lập
			172.16.16.1/24	Port 3	WAN Site to Site
			192.168.1.254/24	Port 4	Kết nối đến Management Switch
				Port 8	Kết nối đến FortiSwitch
			192.168.6.1/24	Port 12	Kết nối FortiSandBox qua VLAN trên CoreSwitch
		VLAN99	172.16.99.254/24	Port14	Kết nối với CoreSwitch
Vùng DMZ					
2	FortiWeb 100D	VLAN 10	192.168.1.251	Port1	Management Port Kết nối với Switch Management
			10.1.1.252/24	Port 2	Kết nối với FortiGate qua Switch DMZ
Vùng WAN					
3	Array APV1800	DC-DC	Virtual IP: 10.10.10.12/24	Port 2	DR-DC WAN
		VLAN 10	192.168.1.240/24	Port 1	Port Management
Vùng CORE					
1	Allied Telesis x550	VLAN99	172.16.99.253/24	Port20	CoreSwitch kết nối FG100E
		VLAN 4 (VLAN- Server)	172.16.4.254/24	Port19	CoreSwitch kết nối FG-80E (VLAN4) (Access VLAN4)
		VLAN 3	172.16.3.254/24	Port 18 (LACP)	CoreSwitch kết nối AccessSwitch User (VLAN2 3 10)
		VLAN 2	172.16.2.254/24		
		VLAN 10	192.168.1.243/24		Port Management
Vùng Internal					
1	FortiGate 80E	VLAN 4	192.168.1.248/24	Port 1	Management Port Kết nối với Switch Management
				Port 5	Kết nối với FortiSwitch
				Port 11	FG80E kết nối Transparent xuống ServerSwitch
				Port 12 (Server SW)	FG80E kết nối Transparent lên CoreSwitch

2	FortiSIEM	VLAN 4	172.16.4.250	Soft-Switch (Port 56789)	ForiSIEM kết nối Mngt SW
		VLAN 10	192.168.1.236		Kết nối đến Mngt SW
3	FortiAuthenticator 200E	VLAN 10	192.168.1.236/24	Port 1	Kết nối với Management Switch
		VLAN 4	172.16.4.249/24	Port 2	Kết nối với Server Switch
4	FortiManager 200F	VLAN 10	192.168.1.235/24	Port1	Kết nối với Management Switch
		VLAN 4	172.16.4.248	Port2	Kết nối với Server Switch
5	FortiSanbox 500F	VLAN 4	172.16.4.247	Port 4	Sanbox kết nối FG80E Mngt SW
		VLAN 10	192.168.1.234	Port 1	Kết nối đến Mngt SW
		VLAN 6	192.168.6.253/24	Port 3	Kết nối lên Port 3 của CoreSW, dành cho VM đi Internet
6	FortiEMS	VLAN 4	172.16.4.246		EMS nằm trong Server VM
8	Server		192.168	Interface GB1	Kết nối đến Mngt SW
9	IDRAC	VLAN10	192.168.1.224	IDRAC	Kết nối đến Mngt SW
10	Vm Exsi	VLAN10	172.16.4.243/24	Interface GB1	Kết nối đến Server SW
11	DVWA		172.16.4.241/24	<u>dvwa.hcm.edu.com</u>	
12	FortiMail 200F	VLAN 4	172.16.4.245/24	port 2	FortiGate kết nối FortiMail
13		VLAN 10	192.168.1.249/24	Port 1	Kết nối đến Mngt SW
14	FortiSwitch 108-1			Port 8	Kết nối Port 6 Fortigate 100E-1
				Port 7	Kết nối Port 6 Fortigate 100E-2
	FortiSwitch 108-2			Port 8	Kết nối Fortigate 80E-1
15	Mail-Server	Vlan 4	172.16.4.242		Nằm trên Server VM

Site DR: được quy hoạch IP và đấu nối như sau:

	Thiết Bị	VLANID	IP	Port	Mô Tả
Vùng Core					
1	FortiGate 80E		192.168.1.253/24	Port 1	Kết nối Management Switch
			172.16.16.2/24	Port 2	WAN Site to Site
			10.1.1.254/24	Port 3	Kết nối FortiWeb
			10.10.10.13/24	Port 4	Mạng DR-DC WAN giả lập
			172.16.100.254/24	Port 12	Kết nối với CoreSwitch
2	CoreSwitch	VLAN 5	172.16.5.253/24	Port 23	CoreSwitch kết nối FG50E Port 5
		VLAN 100	172.16.100.253/24	Port24	Kết nối CoreSW - FG80E
		VLAN 10	192.168.1.241/24	Port1	Kết nối Mngt SW DR

Vùng DMZ					
1	FortiWeb 100D	VLAN 10	192.168.1.250/24	Port1	Port Management Kết nối với Management Switch
			10.2.2.250/24	Port2	Kết nối FortiGate 80E DR
Vùng Internal					
1	FortiGate 50E	VLAN 10	192.168.1.252/24	Port 1	Kết nối với Management Switch
			Transparent	Port 4	Transparent xuống Server Switch
			Transparent	Port 5	Transparent lên CoreSwitch
2	Server Switch			Port 1	ServerSwitch kết nối FG80E (Internal)
		VLAN 10		Port 24	Sw Mgmt DR - Core
	QNAP	VLAN 10	192.168.1.231/24	Port 1	Kết nối với Management Switch
		VLAN5	172.16.5.9/24	Port 2	Kết nối với Server Switch
	Server	Vlan5	172.16.5.243/24	IDRAC	kết nối port 5 sw3 ip 97

5.2 Quy hoạch Port cho hạ tầng Access Switch

5.2.1 Quy hoạch Port trên Switch Access dành cho hệ WAN và Server

Thiết bị Switch ZyXEL 1900 sử dụng tính năng VLAN để phục vụ cho kết nối đến vùng WAN và Server, thông tin phân phối Port như sau:

VLAN ID	VLAN Name	Port	To Port Device	Mode
1	MGMT	1	SW238, Port19	Access
100	Internet 1	2	Internet	Access
100	Internet 1	3	FG100E-1, Port1	Access
100	Internet 1	4	FG100E-2, Port1	Access
200	WAN	5	FG100E-1, Port3	Access
200	WAN	6	FG100E-2, Port3	Access
200	WAN	7	FG80E, Port4	Access
300	DR-DC	8	Array, Port2	Access
300	DR-DC	9	FG100E-1, Port2	Access
300	DR-DC	10	FG100E-2, Port2	Access
300	DR-DC	11	to User test	Access
300	DR-DC	12	FG80E, Port2	Access
4	LAN Server	13	FMG, Port2	Access
4	LAN Server	14	FSA, Port2	Access
4	LAN Server	15	FAC, Port2	Access
4	LAN Server	16	FML, Port2	Access
4	LAN Server	17	FG80E-1, Port11	Access
4	LAN Server	18	FG80E-2, Port11	Access
4	LAN Server	19	SW237, Port2, Vlan4 access	Access
4	LAN Server	20		Access
4	LAN Server	21		Access
4	LAN Server	22		Access

4	LAN Server	23		Access
4	LAN Server	24		Access

--> Thiết bị này còn trống 5 Port phục vụ cho các kết nối của Sinh viên/Giảng viên trực tiếp vào vùng Server (VLAN 4).

5.2.2 Quy hoạch Port trên Switch Access dành cho hệ User và quản trị

Thiết bị switch ZyXEL 1900 phục vụ cho các kết nối từ VLAN User, và vùng quản trị dành riêng cho toàn bộ các thiết bị trong hệ thống (dự phòng các trường hợp lỗi do thao tác thực hành Lab).

Thông tin quy hoạch Port và VLAN như sau:

VLAN ID	VLAN Name	Port	To Port Device	Mode
2	User VLAN 2	1	Wifi User (Engenius AP)	Access
2	User VLAN 20 (test)	2	[Dùng cho Lab, sinh viên cắm cáp vào]	Access
3	User VLAN 30 (test)	3	[Dùng cho Lab, sinh viên cắm cáp vào]	Access
3		4	[Dùng cho Lab, sinh viên cắm cáp vào]	Access
20	DMZ-Fortiweb	5	FG100E-2, DMZ	Access
20	DMZ-Fortiweb	6	FG100E-1, DMZ	Access
20	DMZ-Fortiweb	7	FortiWeb, Port2	Access
10	MGMT	8	Fortigate 80E, Port1	Access
10	MGMT	9	Fortigate 80E-2, Port1	Access
10	MGMT	10	MGMT Wifi	Access
10	MGMT	11	Fortiweb100D, Port1	Access
10	MGMT	12	FSA Port1	Access
10	MGMT	13	Fmail Port1	Access
10	MGMT	14	Coresw1, Port1	Access
10	MGMT	15	Coresw2, Port1	Access
10	MGMT	16	Array, Port1	Access
10	MGMT	17	FAC-Port1	Access
10	MGMT	18	to MGMT Vlan 10, SW DR, Port11	Access
10	MGMT	19	SW239, Port1	Access
10	MGMT	20	FMG, Port1	Access
10	MGMT	21	FG100E-2, Port4	Access
10	MGMT	22	FG100E-1, Port4	Access
		23	LACP-Core - Core2	Trunk
		24	LACP-Core - Core1	Trunk

--> Thiết bị này còn trống các Port 2, 3, 4 phục vụ cho kết nối LAN User (dùng kết nối ra Jump Port cho Sinh viên kết nối vào).

5.2.3 Quy hoạch Port trên Switch Access dành cho Site DR

VLAN ID	VLAN Name	Port	To Port Device	Mode
1		1	To Server Trunk, vlan 10, 4	Trunk
4	VLAN 4	2	To SW239, Port19	Access
4	VLAN 5	3	QNAP, Port2	Access
5	VLAN 5	4	FG50E, Port4	Access

5	VLAN 5	5		Access
5	VLAN 5	6	Server Port 2	Access
5	VLAN 5	7		Access
10	VLAN 10	8		Access
10	VLAN 10	9	FG50E, Port1	Access
10	VLAN 10	10	CoreSW-DR, Port1	Access
10	VLAN 10	11	SW238, Port18	Access
10	VLAN 10	12	QNAP, Port1	Access
10	VLAN 10	13	FG80E-DR, Port1	Access
10	VLAN 10	14	FWB10D-DR, Port2	Access
10	VLAN 10	15	FAP1	Access
10	VLAN 10	16	FAP2	Access
10	VLAN 10	17		Access
10	VLAN 10	18	Server	Access
		19		
		20		
		21		
		22		
		23		
		24		

--> Thiết bị này gồm cả phần VLAN quản trị của site DR và VLAN 4 (Server site DC), VLAN 5 (Server site DR). Do 2 hệ thống sử dụng chung chung Server.
Các Port còn lại từ 19 đến 24 được linh hoạt sử dụng theo nhu cầu sau này của trường.

5.3 IP Quản trị hệ thống

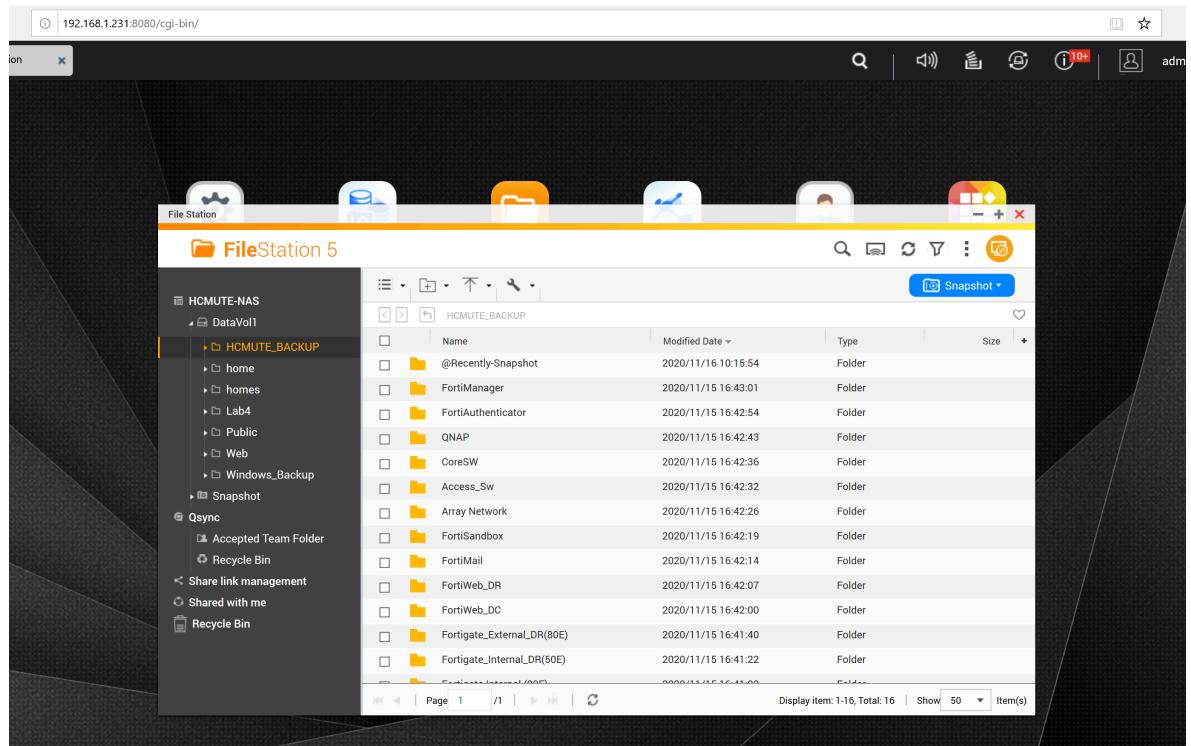
Thiết bị	IP Quản trị	Account Quản trị	Cách quản trị
FG-100E-DC	https://192.168.1.254	student student@123	Quản trị qua Web
FG-80E-DC	https://192.168.1.248	student student@123	Quản trị qua Web
FG-80E-DR	https://192.168.1.253	student student@123	Quản trị qua Web
FG-50E-DR	https://192.168.1.252	student student@123	Quản trị qua Web
FortiMail	https://192.168.1.249/admin	student student@123	Quản trị qua Web (/admin)
FortiWeb 100D-DC	https://192.168.1.251	student student@123	Quản trị qua Web
FortiWeb 100D-DR	https://192.168.1.250	student student@123	Quản trị qua Web
Array	https://192.168.1.240:8888	student array	Quản trị qua Web (Port 8888)
CoreSwitch - DC	Pri:192.168.1.243	student	Putty Console, Telnet, hoặc Web

		alliedtelesis@123	
CoreSwitch - DR	Pri:192.168.1.241	student alliedtelesis@123	Putty Console, Telnet, hoặc Web
Access SW WAN + Server	https://192.168.1.239	student zyxel@123	Quản trị qua Web
Access SW User + Mngt	https://192.168.1.238	student zyxel@123	Quản trị qua Web
Access SW DR	https://193.168.1.237	student zyxel@123	Quản trị qua Web
Engenius MGMT	SSID: MGMT Wifi Password: Mgmt@123	admin admin	Quản trị qua Web
Engenius User	SSID: User VLAN Password: User@123	admin admin	Quản trị qua Web
FortiAuthenticator	https://192.168.1.236	student student@123	Quản trị qua Web
FortiManager	https://192.168.1.235	student student@123	Quản trị qua Web
FortiSanbox	https://192.168.1.234	student student@123	Quản trị qua Web
FortiEMS	https://172.16.4.246	student student@123	Quản trị qua Web
FortiSIEM	https://172.16.4.250	student student@123	Quản trị qua Web
QNAP	https://192.168.1.231	student student@123	Quản trị qua Web
FortiAP (Tài khoản mặc định)	https://192.168.1.2	admin Pass để trống	
FortiSW1			Quản trị qua Fortigate
FortiSW2			Quản trị qua FortiGate
DVWA1(DC)	https://172.16.4.238	admin/password	Quản trị qua Web
DVWA2(DC)	https://172.16.4.241	admin/password	Quản trị qua Web
DVWA DR	https://172.16.4.241	admin/password	Quản trị qua Web
Test PC	RDP: 172.16.4.71	tp\P@ssword	Quản trị bằng RDP
DNS	RDP: 172.16.4.242	Administrator\P@ssword	Quản trị bằng RDP

6 Các hướng dẫn

6.1 Hướng dẫn khôi phục hệ thống

Lưu ý: toàn bộ các file Backup cấu hình của hệ thống ở trạng thái hoạt động ổn định (hoạt động toàn bộ hạ tầng, chưa bao gồm các cấu hình của các bài Lab) được lưu trữ trên thư mục của QNAP:



6.1.1 Zyxel

Factory Reset

Bấm và giữ nút RESET nằm ở mặt trước thiết bị khoảng 15-20s

Chờ thiết bị khởi động lại, đặt IP máy tính là 192.168.1.11/24

Kết nối máy tính với Port 1 trên Switch GS1900-24HP

Truy cập vào địa chỉ IP mặc định <https://192.168.1.1>

Username: admin

Password: ****

Backup cấu hình:

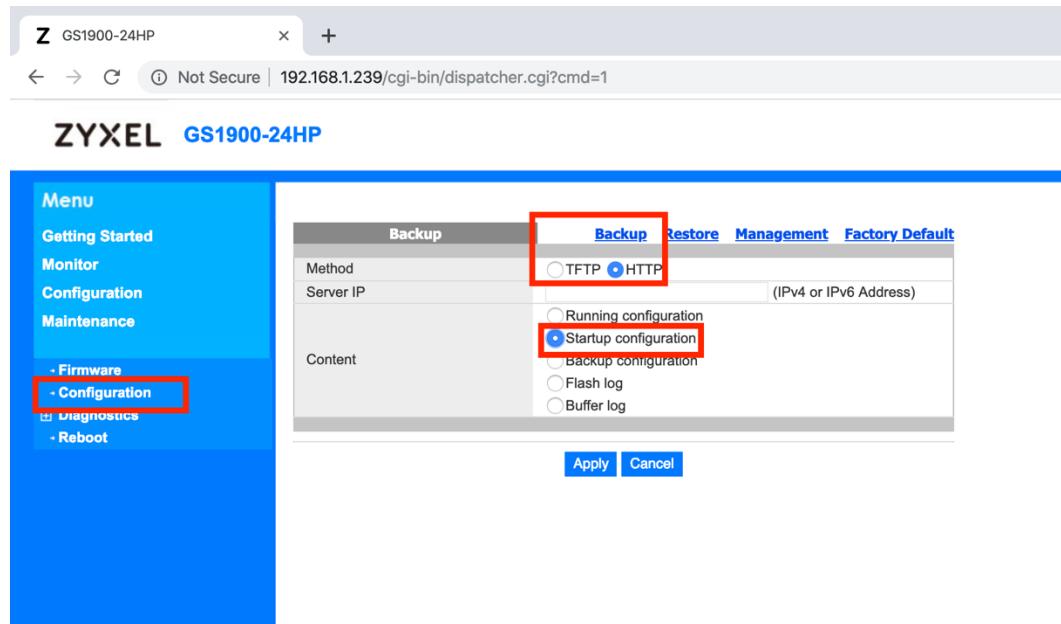
Truy cập vào các thiết bị Switch-Access Zyxel bằng trình duyệt (ưu tiên FireFox) theo địa chỉ:

192.168.1.237

192.168.1.238

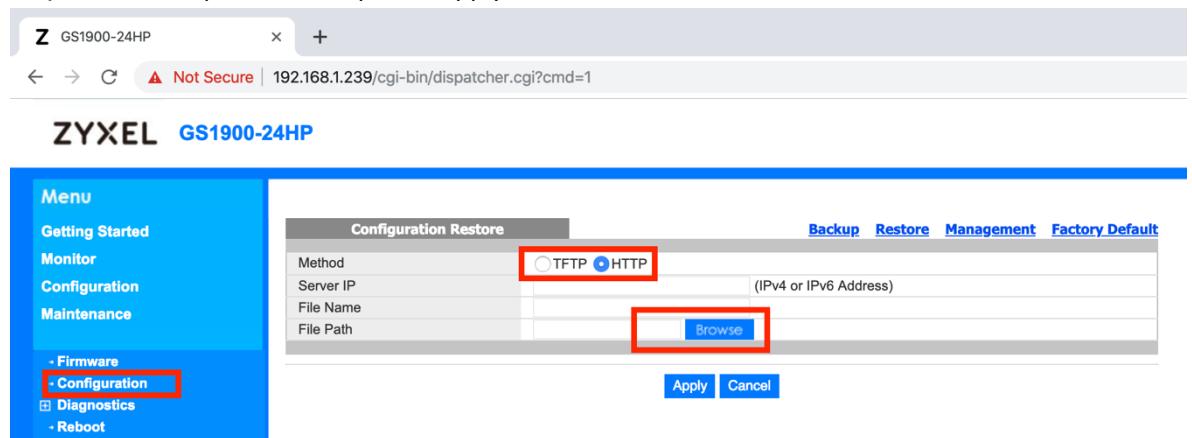
192.168.1.239

Maintenance > Configuration > Backup



Restore cấu hình:

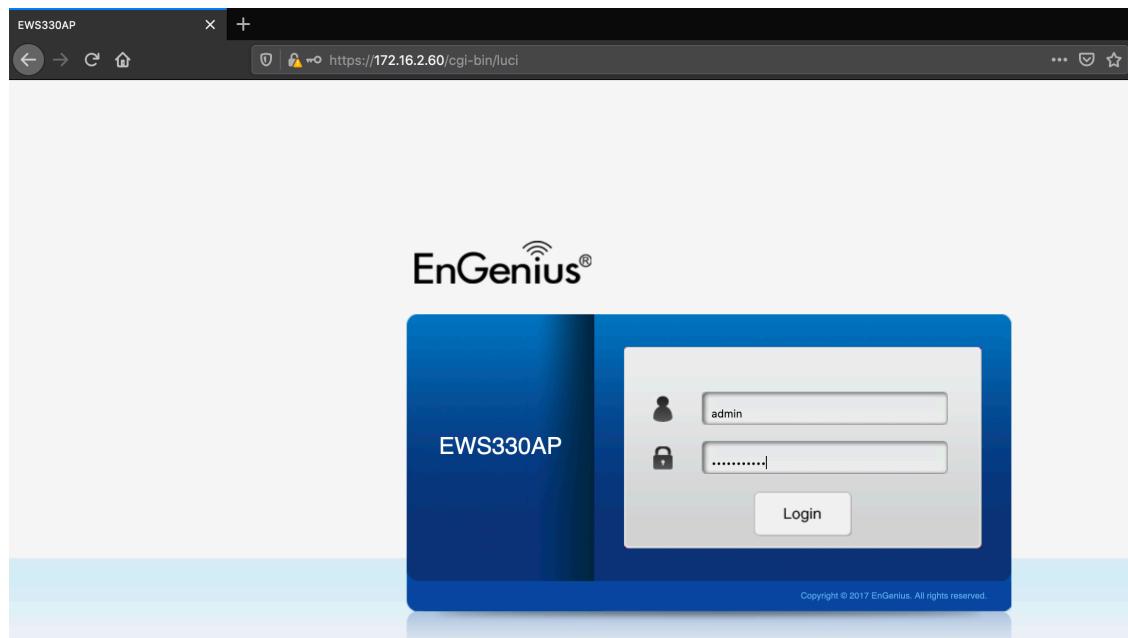
Maintenance > Configuration > Restore
Chọn File Backup đã lưu > Open > Apply



6.1.2 Engenius

Factory Reset

Nhấn và giữ nút Reset nằm ở mặt dưới thiết bị khoảng 20-30s.
Chờ thiết bị khởi động lại, đặt IP máy tính là 192.168.1.11/24
Kết nối máy tính với Port LAN ở mặt dưới Engenius EWS330AP
Truy cập vào địa chỉ IP mặc định https://192.168.1.1
Username: admin
Password: ****



Cấu hình SSID:

Network > Basic > DHCP mode > Save

Network > Wireless > Wireless Setting 2.4GHz và 5GHz điền SSID User WiFi > Edit

Enabled	SSID	Edit	Security
<input checked="" type="checkbox"/>	User WiFi	Edit	WPA2/PSK TKIP+AES
<input type="checkbox"/>	EnGenius721852_2-2.4GHz	Edit	None
<input type="checkbox"/>	EnGenius721852_3-2.4GHz	Edit	None
<input type="checkbox"/>	EnGenius721852_4-2.4GHz	Edit	None
<input type="checkbox"/>	EnGenius721852_5-2.4GHz	Edit	None
<input type="checkbox"/>	EnGenius721852_6-2.4GHz	Edit	None
<input type="checkbox"/>	EnGenius721852_7-2.4GHz	Edit	None
<input type="checkbox"/>	EnGenius721852_8-2.4GHz	Edit	None

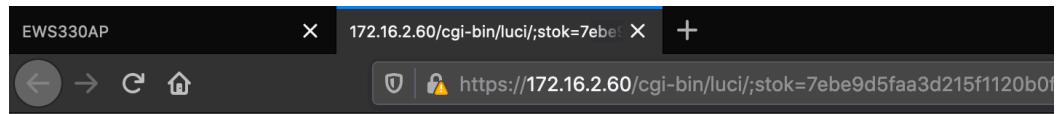
Enabled	SSID	Edit	Security
<input checked="" type="checkbox"/>	User WiFi	Edit	WPA2/PSK TKIP+AES
<input type="checkbox"/>	EnGenius721853_2-5GHz	Edit	None
<input type="checkbox"/>	EnGenius721853_3-5GHz	Edit	None

Security Mode: WPA2-PSK

Encryption: Both(TKIP+AES)

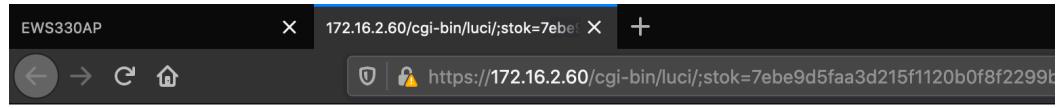
Passphrase: Mật khẩu Wifi

Save để lưu



Wireless Security - 2.4GHz

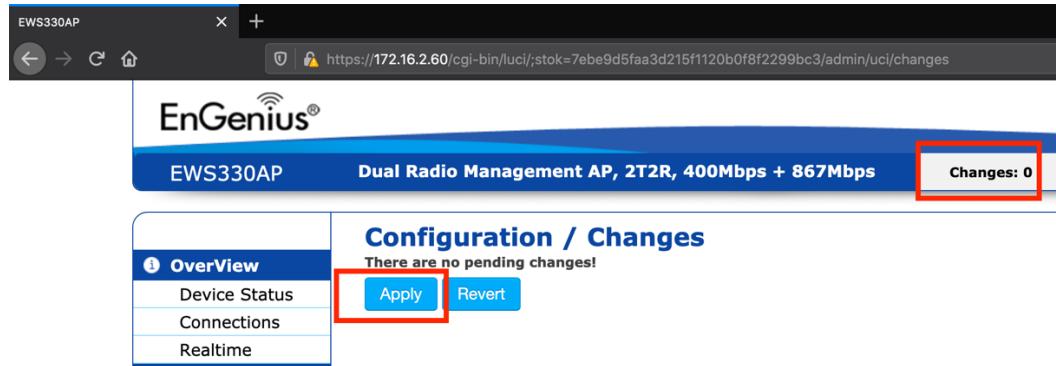
Security Mode	WPA2-PSK
Encryption	Both(TKIP+AES)
Passphrase	User@123
Group Key Update Interval	3600



Wireless Security - 5GHz

Security Mode	WPA2-PSK
Encryption	Both(TKIP+AES)
Passphrase	User@123
Group Key Update Interval	3600

Chọn Changes > Apply để áp dụng cấu hình vừa tạo.



Backup

System management > Firmware > Backup Setting (Factory Setting) > Export

EnGenius®

EWS330AP Dual Radio Management AP, 2T2R, 400Mbps + 867Mbps Changes: 0

Network

Management

System Manager

Firmware

Firmware Upgrade

Current Firmware Version: 3.5.1

Select the new firmware from your hard disk.

No file selected.

Backup/Restore Settings

Factory Setting

- Backup Setting

- Restore New Setting No file selected.

- Reset to Default

User Setting

- Back Up Setting as Default

- Restore to User Default

Warning: This feature will overwrite the factory default setting with your current AP settings. A physical reset button will restore the configuration of the current AP settings, not factory restore to factory settings, press Factory Setting, Reset to Default in the UI.

Restore

System management > Firmware > Restore New Setting (Factory Setting) > Browse (chọn file backup) > Import

EnGenius®

EWS330AP Dual Radio Management AP, 2T2R, 400Mbps + 867Mbps Changes: 0

Network

Management

System Manager

Firmware

Firmware Upgrade

Current Firmware Version: 3.5.1

Select the new firmware from your hard disk.

No file selected.

Backup/Restore Settings

Factory Setting

- Backup Setting

- Restore New Setting No file selected.

- Reset to Default

User Setting

- Back Up Setting as Default

- Restore to User Default

Warning: This feature will overwrite the factory default setting with your current AP settings. A physical reset button will restore the configuration of the current AP settings, not factory restore to factory settings, press Factory Setting, Reset to Default in the UI.

6.1.3 Allied Telesis

LOGIN:

Cách 1:

Login trực tiếp bằng cable Console (cắm trực tiếp cable Console từ PC, Laptop vào Port Console trên thiết bị)

Mở phần mềm PUTTY.

Serial Line: COMX (kiểm tra tại manage computer)

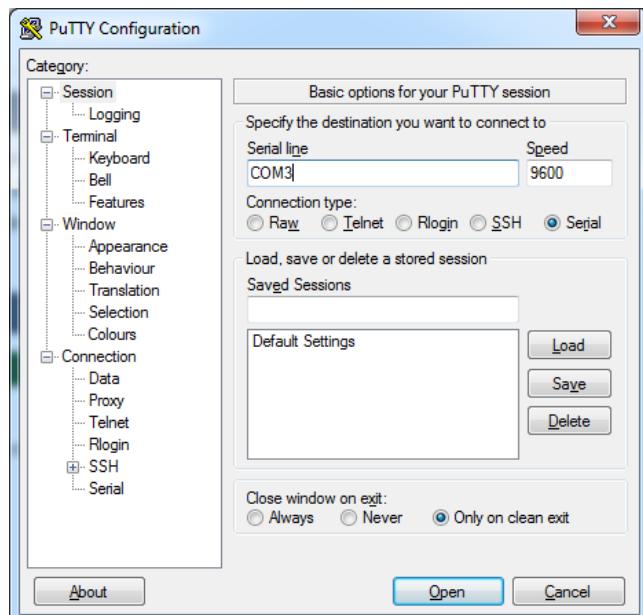
Bit per second: 9600

Data bit: 8

Parity: none

Stop bit: 1

Flow control: none

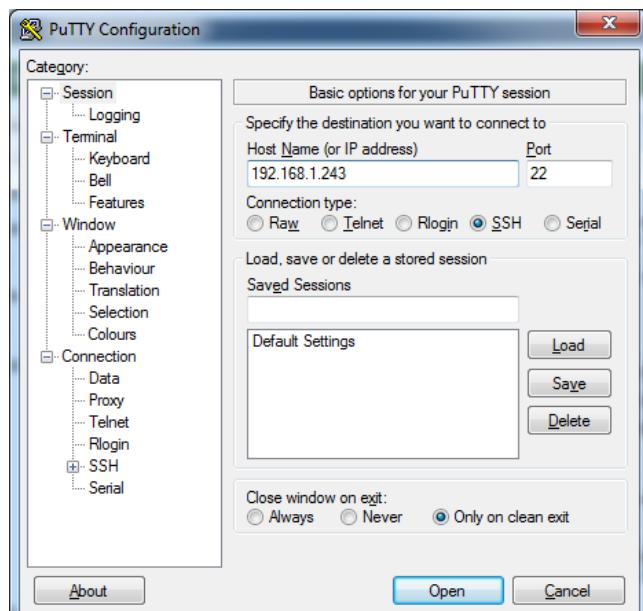


Cách 2:

Login bằng phần mềm PUTTY (SSH):
192.168.1.243

Username: manager

Password: friend



Factory Reset

Login vào giao diện CLI

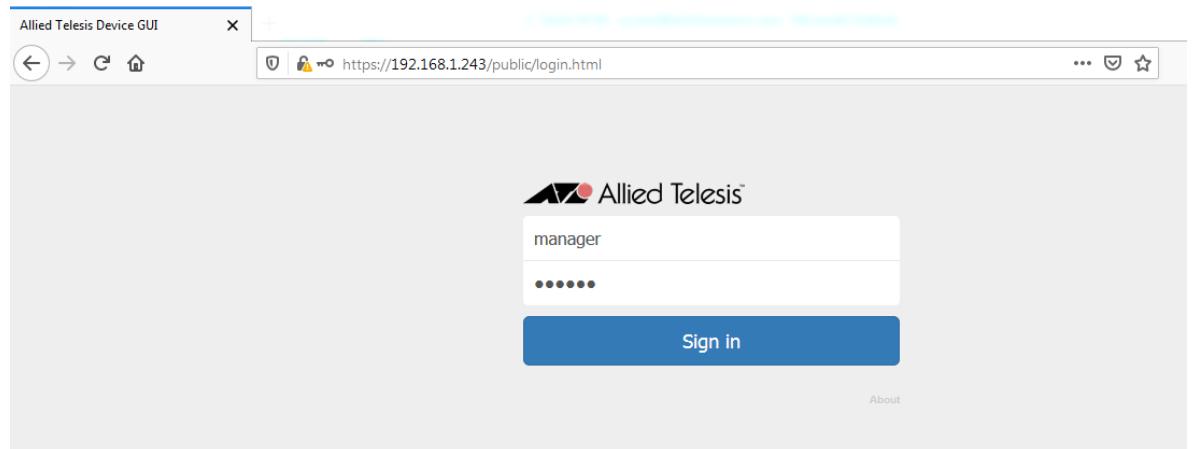
```
Awplus# erase factory-default
```

Backup

Kết nối với Wifi MGMT > truy cập vào trình duyệt với địa chỉ 192.168.1.243

Username: manager

Password: *****



System > File Management > Download File Backup

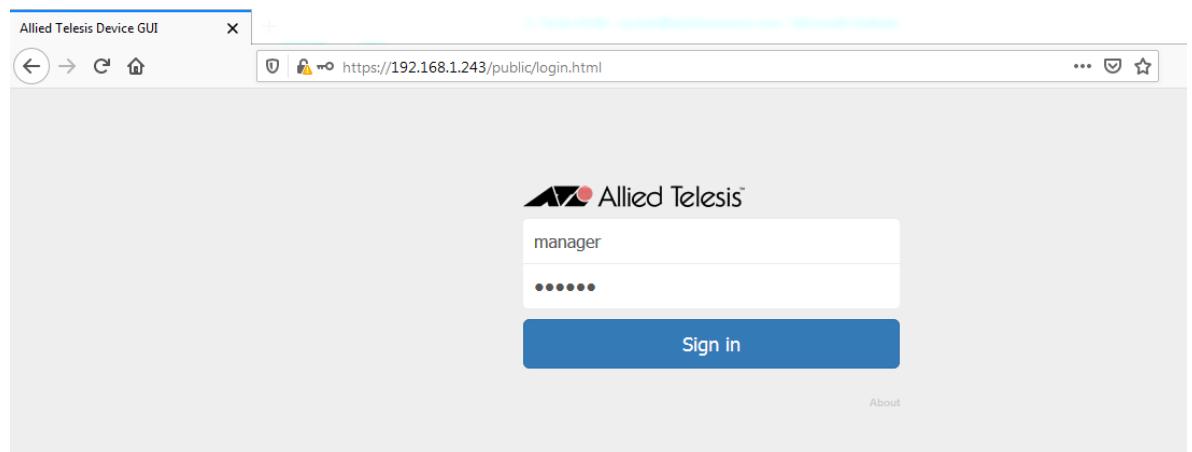
Name	Modified	Size(bytes)	Actions
awplus-gui_549_13....	1/10/2020, 10:25:53 AM	2265088	Download Delete
default.cfg	11/15/2020, 3:38:24 PM	4647	Download Delete
gui-userdata	10/24/2020, 1:54:36 PM		
log	11/15/2020, 12:40:00 PM		

Restore

Kết nối với Wifi MGMT > truy cập vào trình duyệt với địa chỉ 192.168.1.243

Username: manager

Password: *****



System > File Management > Upload File Backup

Set Boot Config File > chọn file Backup (Backup16-11) > Apply
 Sau đó tiến hành Reboot thiết bị

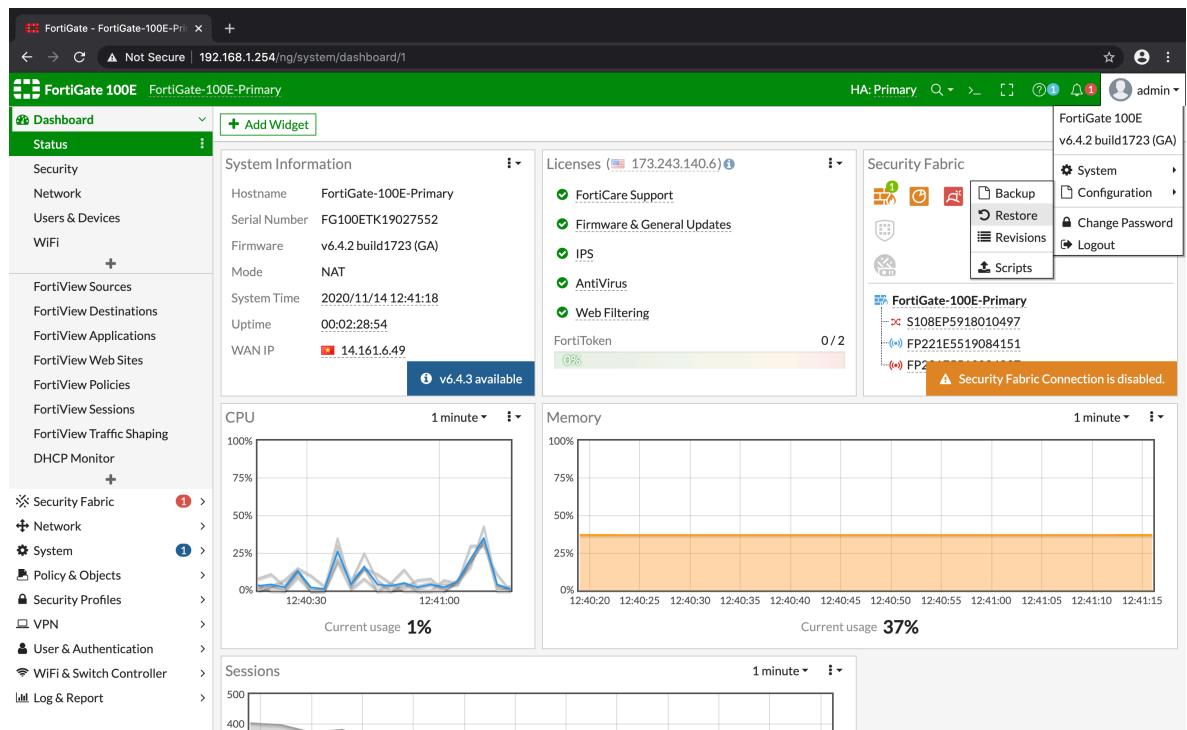
*Đối với trường hợp không Login vào được Giao diện Web

Login vào CLI

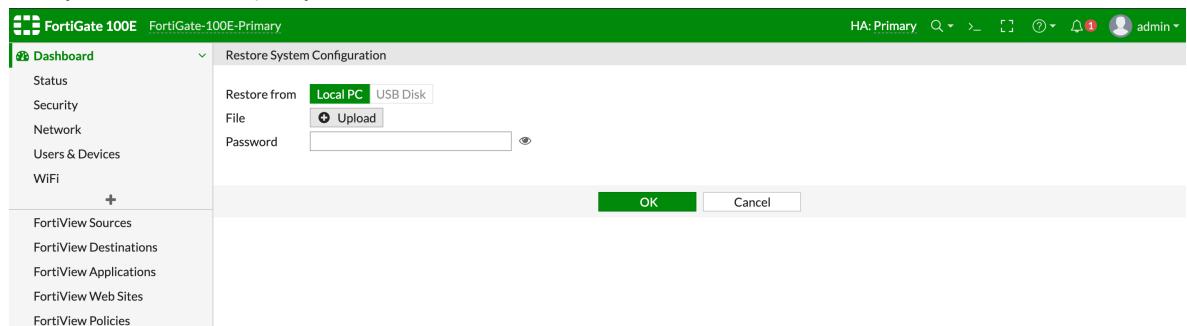
```
Awplus# configure terminal
Awplus(config)# boot config-file flash:/backup16-11.cfg
Awplus(config)# exit
Awplus# reboot
```

6.1.4 Các thiết bị Fortigate

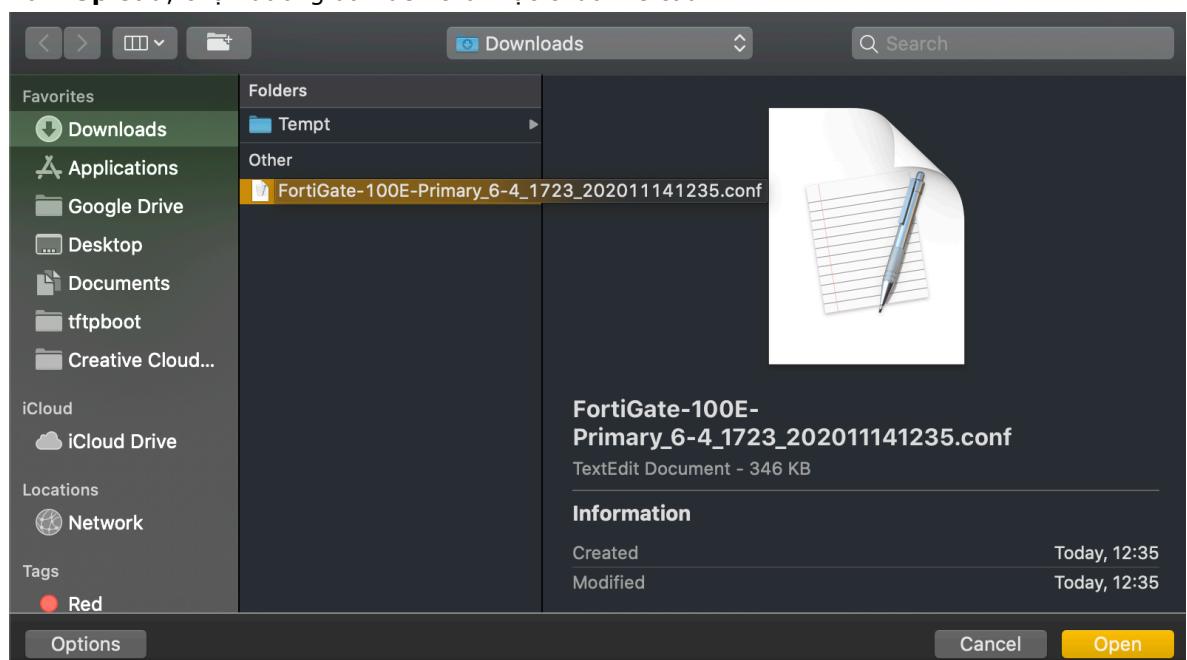
Đăng nhập vào thiết bị FortiGate. Ở giao diện **Dashboard**, bấm vào tài khoản “admin” phía góc phải phía trên. Chọn **Configuration > Restore**:



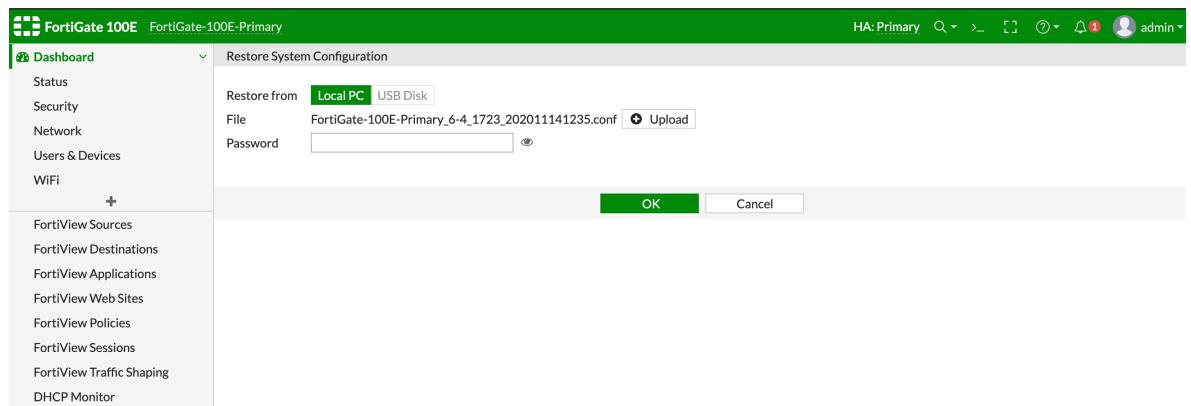
Ở mục Restore from, chọn **Local PC**.



Bấm **Upload**, chọn đường dẫn đến thư mục chứa file cấu hình.



Nếu file cấu hình được mã hóa lúc sao lưu, điền Password đã mã hóa, sau đó bấm OK.
Nếu file cấu hình không được mã hóa lúc sao lưu, Bấm OK.



Quá trình khôi phục cấu hình của FortiGate sẽ được tiến hành.

Fortigate sẽ khởi động lại trong thời gian khôi phục cấu hình.

6.1.5 Thiết bị FortiWeb

Đăng nhập vào thiết bị FortiWeb, truy cập **System > Maintenance > Backup & Restore > Backup & Restore**.

Chọn Restore. Bấm Upload, chọn đường dẫn đến file cấu hình của FortiWeb đã được sao lưu.

Bấm Restore, quá trình khôi phục cấu hình của FortiWeb sẽ được tiến hành. Trong quá trình khôi phục cấu hình, FortiWeb sẽ khởi động lại.

6.1.6 Thiết bị FortiAuthenticator

Đăng nhập vào thiết bị FortiAuthenticator:

Ở giao diện **Dashboard**, bấm vào tên tài khoản phía góc phải phía trên. Chọn **Restore/Backup**:

The screenshot shows the FortiAuthenticator 200E interface with the URL 192.168.1.236. The top right corner shows a user profile with the name 'student'. Below the profile, a dropdown menu is open with options: Upgrade, Restore/Backup (which is highlighted in blue), Reboot, Shutdown, and Logout. The main content area displays 'System Information' and 'User Inventory' tables.

Bấm **Upload a file**, chọn đường dẫn đến thư mục chứa file cấu hình cần khôi phục:

The screenshots show the 'Configuration Backup and Restore' page. The first screenshot shows the 'Backup' section with a 'Download Backup File' button. The second screenshot shows the 'Restore' section with a 'Restore file:' input field containing the file path 'FAC200E-v6.2.1-build0552_1...' and a 'Restore' button.

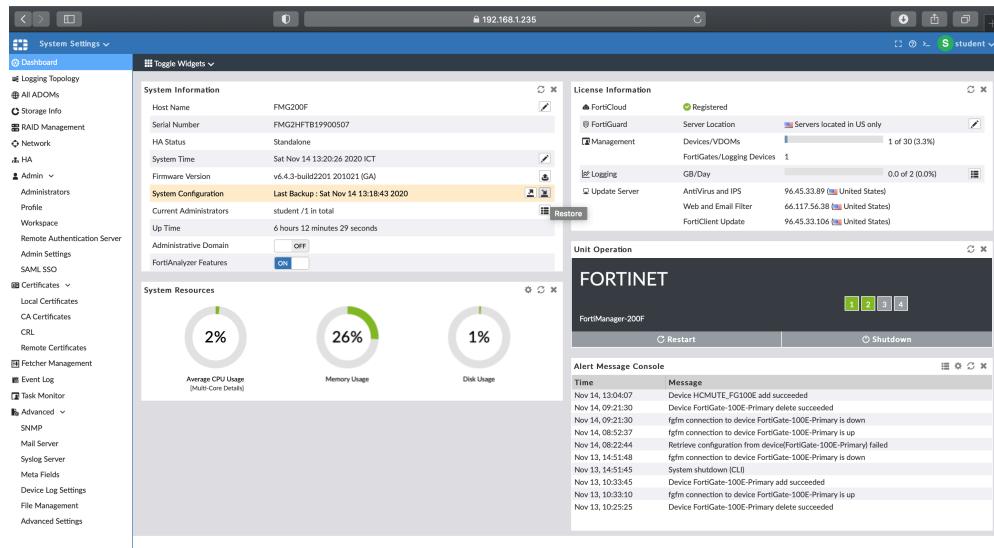
Bấm **Restore**, quá trình khôi phục cấu hình sẽ bắt đầu. Trong quá trình khôi phục cấu hình, FortiAuthenticator sẽ khởi động lại.

6.1.7 Thiết bị FortiManager

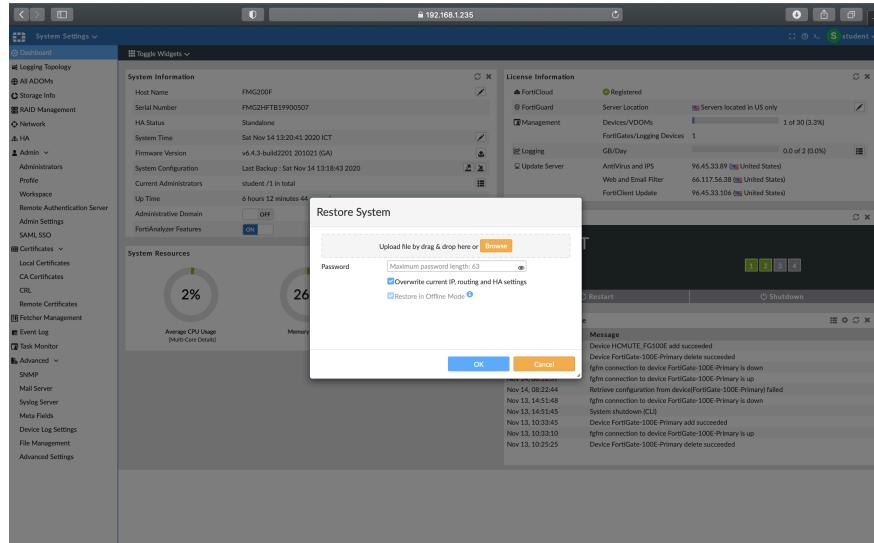
Đăng nhập vào thiết bị FortiManager:

Chọn **System Settings**:

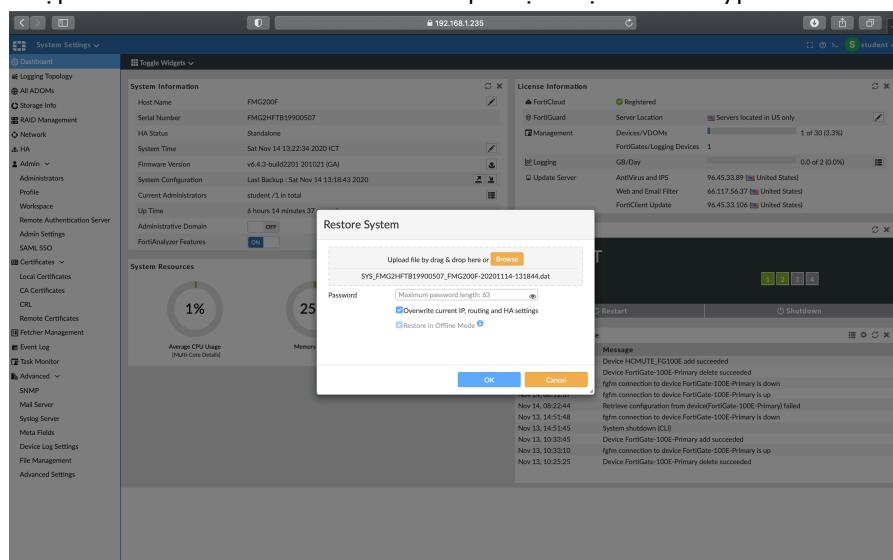
Ở giao diện Dashboard, mục **System Information > System Configuration**, chọn nút **Restore**.



Chọn đường dẫn đến thư mục chứa file cấu hình hoặc kéo thả file cấu hình vào khung **Upload file by drag & drop here or Browse.**



Nhập Password nếu trước đó file backup được chọn mã encryption.

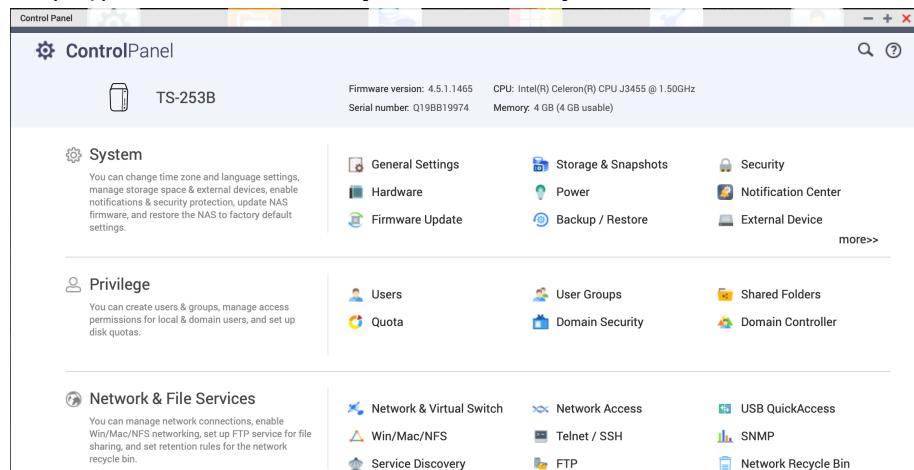


Bấm OK. Quá trình khôi phục cấu hình sẽ bắt đầu, trong quá trình khôi phục cấu hình, FortiManager sẽ khởi động lại.

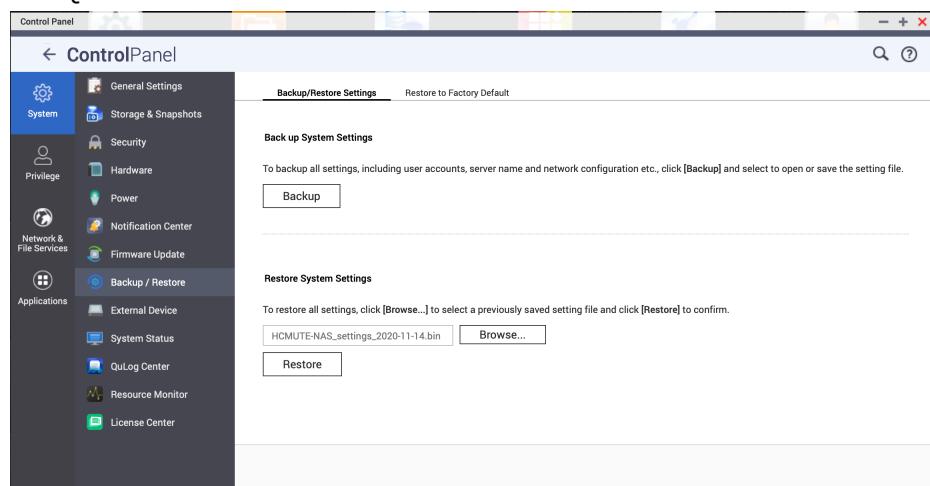
6.1.8 Thiết bị QNAP

Đăng nhập vào thiết bị QNAP:

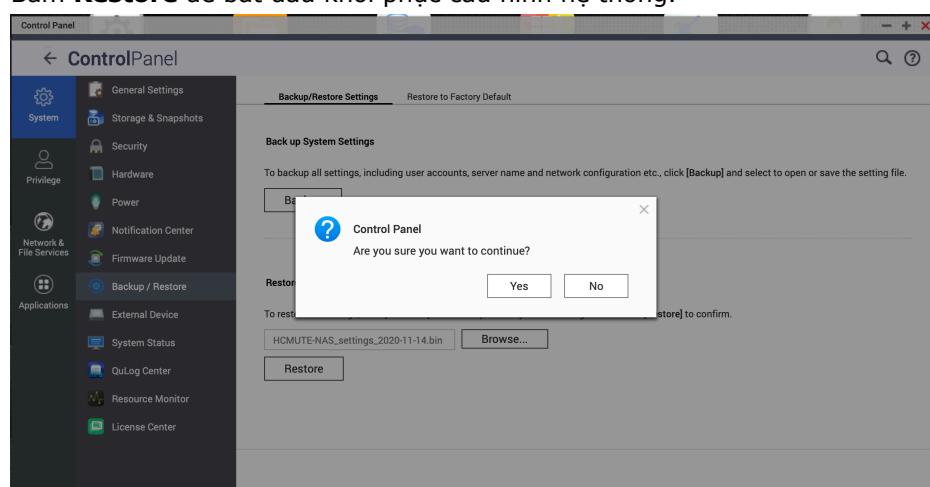
Truy cập **Control Panel > System > Backup / Restore.**



Ở mục Restore System Settings, chọn đường dẫn đến thư mục chứa file cấu hình hệ thống của QNAP.



Bấm **Restore** để bắt đầu khôi phục cấu hình hệ thống.



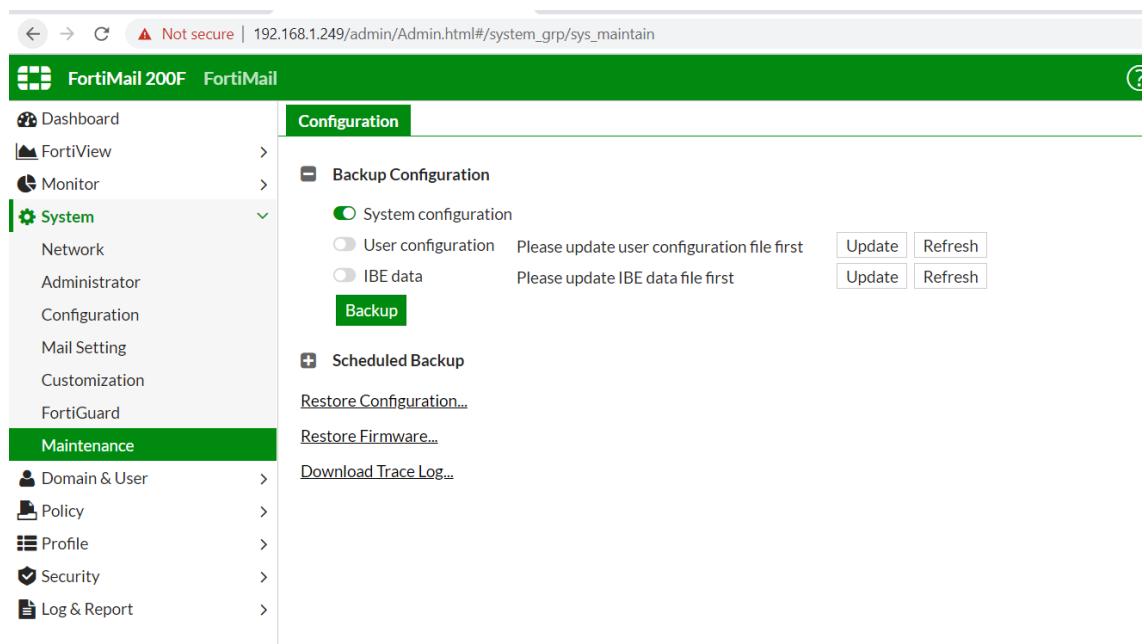
Chọn Yes, QNAP sẽ bắt đầu quá trình khôi phục các cấu hình hệ thống. Trong quá trình này, QNAP sẽ khởi động lại.

6.1.9 Thiết bị FortiMail

Đăng nhập vào thiết bị FortiMail:

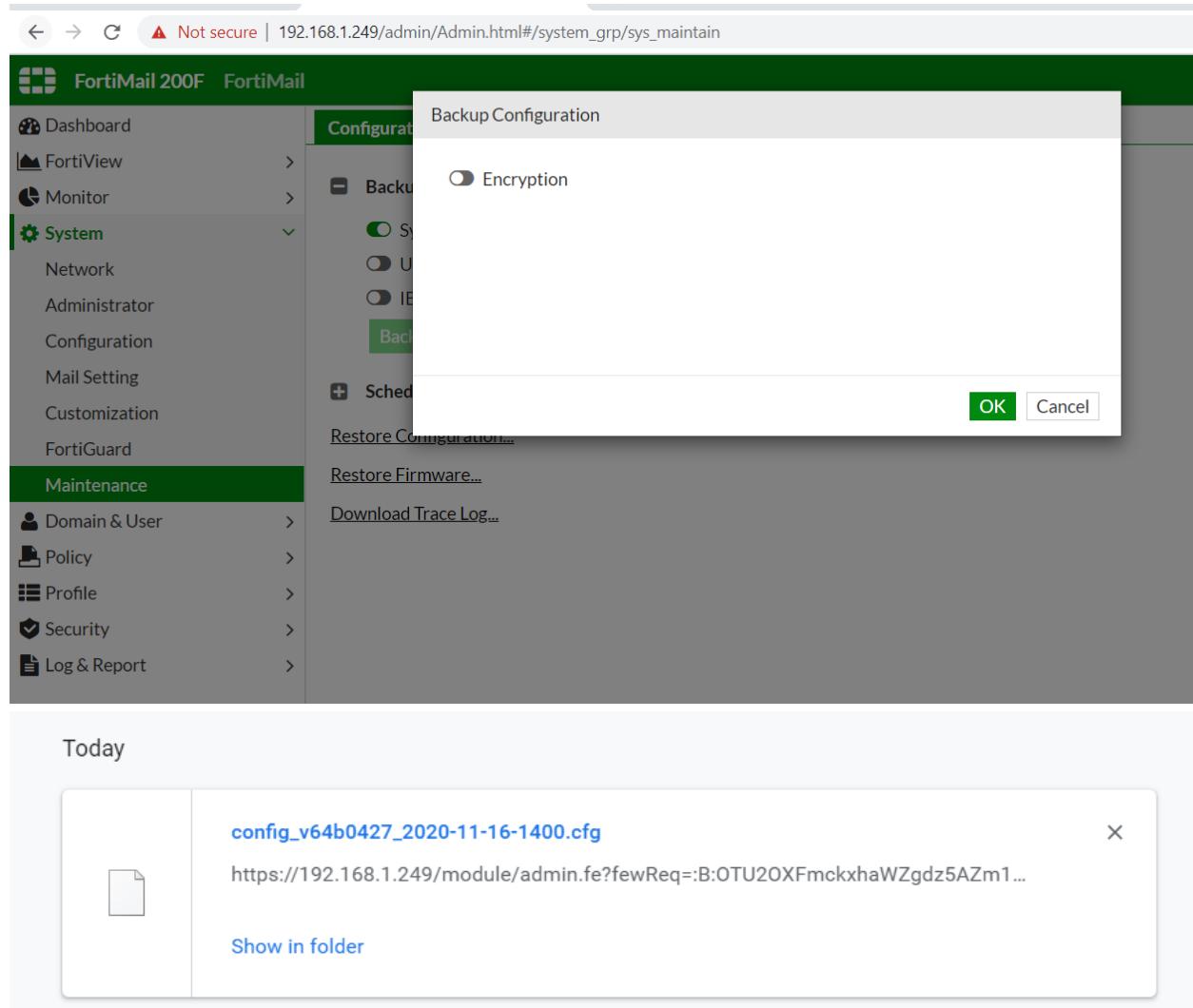
Ở giao diện **Dashboard**, bấm vào tài khoản “admin” phía góc phải phía trên. Chọn **Dashboard ! System -> Maintenance**

Chọn **Update User Configuration và IBE data ! Backup**



The screenshot shows the FortiMail 200F web interface. The URL in the address bar is 192.168.1.249/admin/Admin.html#/system_grp/sys_maintain. The main content area is titled 'Configuration' and contains a 'Backup Configuration' section. In this section, the 'System configuration' radio button is selected, while 'User configuration' and 'IBE data' are disabled. Buttons for 'Update' and 'Refresh' are present. Below this is a 'Scheduled Backup' section with links for 'Restore Configuration...', 'Restore Firmware...', and 'Download Trace Log...'. The left sidebar has a 'System' section with 'Configuration' selected, and a 'Maintenance' section with 'Domain & User', 'Policy', 'Profile', 'Security', and 'Log & Report' listed. The 'Configuration' and 'Maintenance' sections are highlighted in green.

Bấm **OK**. File cấu hình hiện tại của thiết bị sẽ được tải xuống máy tính.



Not secure | 192.168.1.249/admin/Admin.html#/system_grp/sys_maintain

FortiMail 200F FortiMail

Dashboard

FortiView

Monitor

System

- Network
- Administrator
- Configuration
- Mail Setting
- Customization
- FortiGuard

Maintenance

- Domain & User
- Policy
- Profile
- Security
- Log & Report

Backup Configuration

Encryption

OK Cancel

Restore Configuration...

Restore Firmware...

Download Trace Log...

Today

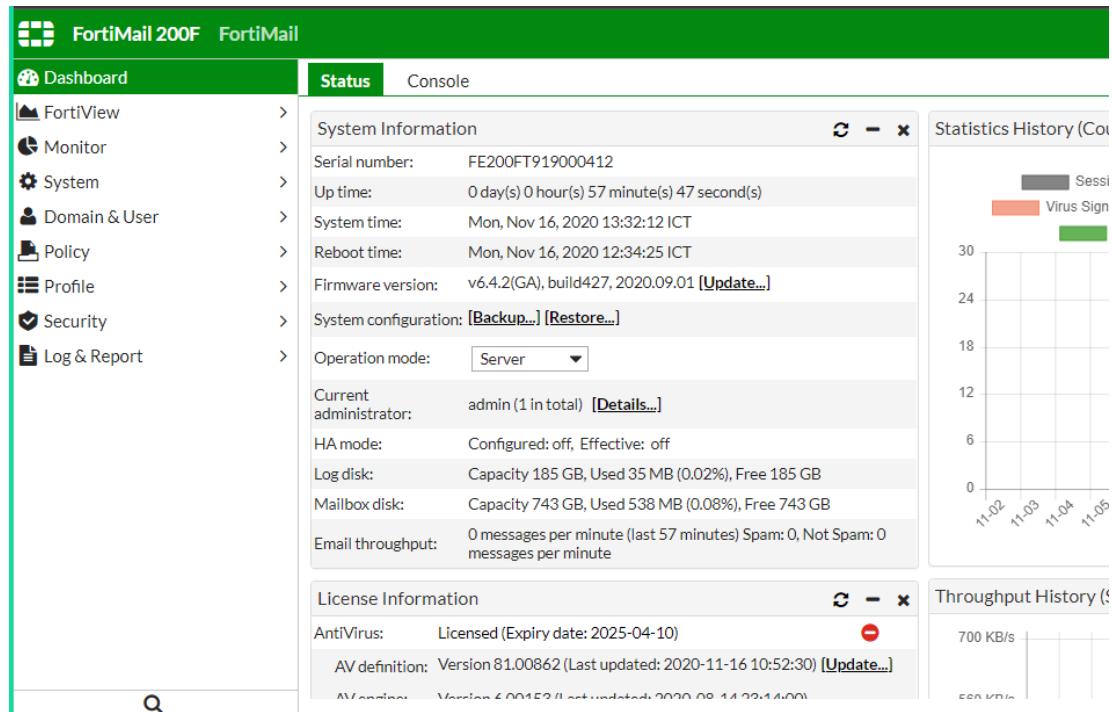
config_v64b0427_2020-11-16-1400.cfg

https://192.168.1.249/module/admin.fe?fewReq=:B:OTU2OXFmckxhaWZgdz5AZm1...

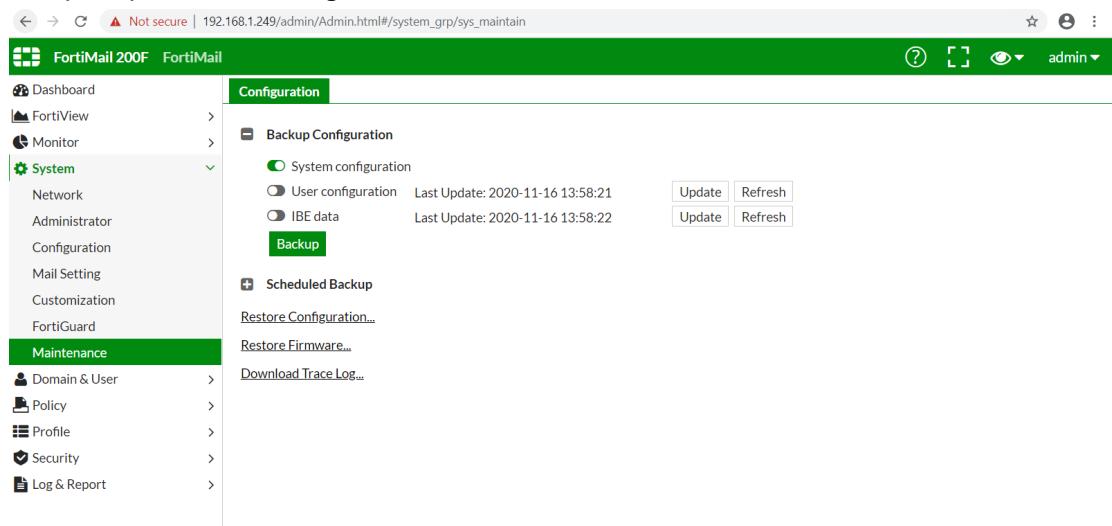
Show in folder

Hướng dẫn khôi phục lại cấu hình của thiết bị FortiMail:

Đăng nhập vào thiết bị FortiGate. Ở giao diện **Dashboard**, bấm vào tài khoản “admin” phía góc phải phía trên. Chọn **Dashboard ! System -> Maintenance**



Ở mục chọn Restore Configuration



Bấm **Upload**, chọn đường dẫn đến thư mục chứa file cấu hình.

	Name	Date modified	Type	Size
Quick access				
Desktop	config_v64b0427_2020-11-16-1400.cfg	16/11/2020 2:03 PM	CFG File	39 KB
Downloads	Bảng thông tin truy cập vào các thiết bị	16/11/2020 1:56 PM	Microsoft Word Document	20 663 KB
Earlier this month (1)				

Nếu file cấu hình được mã hóa lúc sao lưu, điền Password đã mã hóa, sau đó bấm OK.

Nếu file cấu hình không được mã hóa lúc sao lưu, Bấm OK.

Quá trình khôi phục cấu hình của FortiMail sẽ được tiến hành.
FortiMail sẽ khởi động lại trong thời gian khôi phục cấu hình.

6.1.10 Thiết bị FortiSandbox

Đăng nhập vào thiết bị FortiSandbox, truy cập **System > System Recovery > Restore**

Chọn Choose File. Bấm Upload, chọn đường dẫn đến file cấu hình của FortiSandBox đã được sao lưu.

Bấm Restore, quá trình khôi phục cấu hình của FortiSandBox sẽ được tiến hành. Trong quá trình khôi phục cấu hình, FortiSandBox sẽ khởi động lại.

6.1.11 Thiết bị FortiEMS

Đăng nhập vào thiết bị FortiEMS:

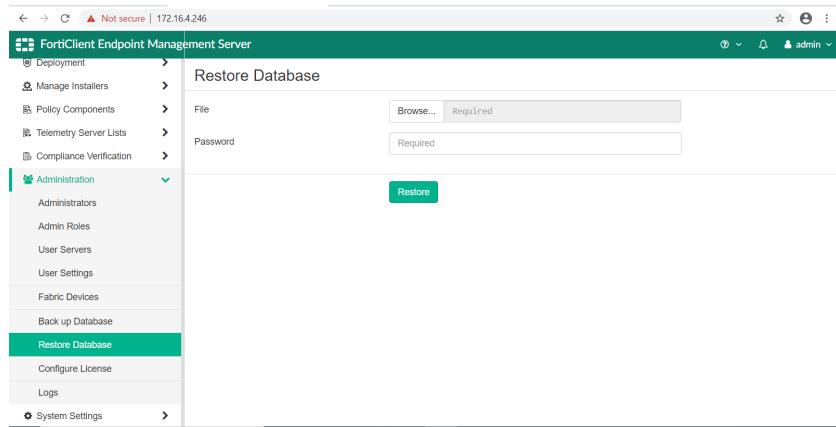
Ở giao diện **Administrator ! Backup Database**

Nhập password và bấm vào nút **Backup** để tải file backup về máy tính.

Thiết bị FortiClient EMS

Tương tự đối với Restore

Ở giao diện Administrator ! Restore Database



Bấm **Browse**, chọn đường dẫn đến thư mục chứa file cấu hình cần khôi phục:

Điền password

Bấm **Restore**, quá trình khôi phục cấu hình sẽ bắt đầu. Trong quá trình khôi phục cấu hình, FortiEMS sẽ khởi động lại.

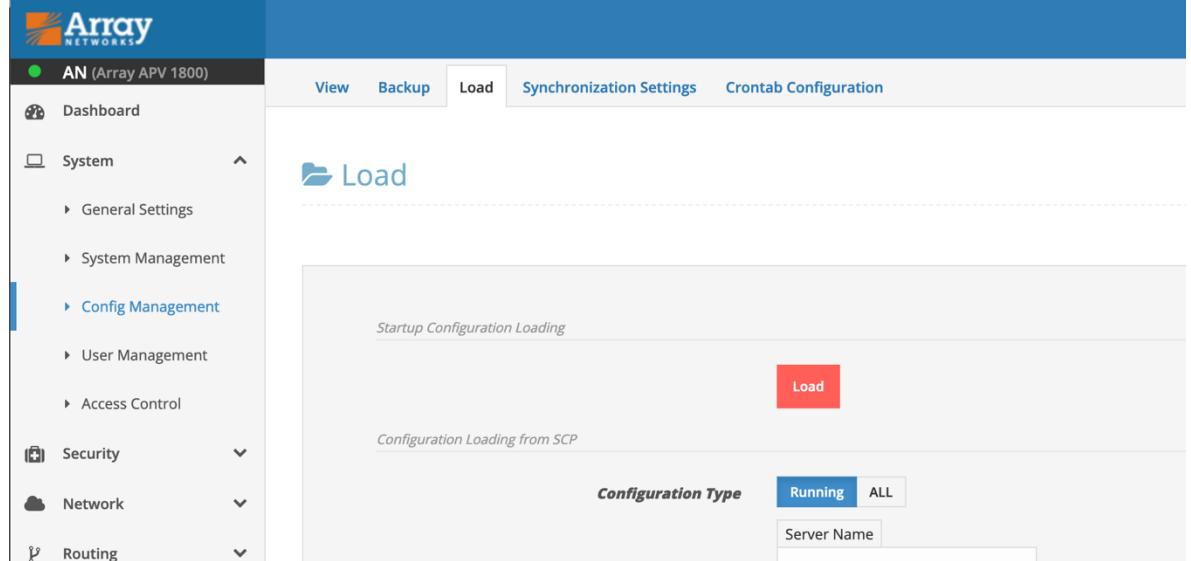
6.1.12 Thiết bị FortiSIEM

Vì đây là thiết bị ảo hóa vui lòng xem qua tài liệu quản trị VM ESX. Để biết cách snapshot các bản VM

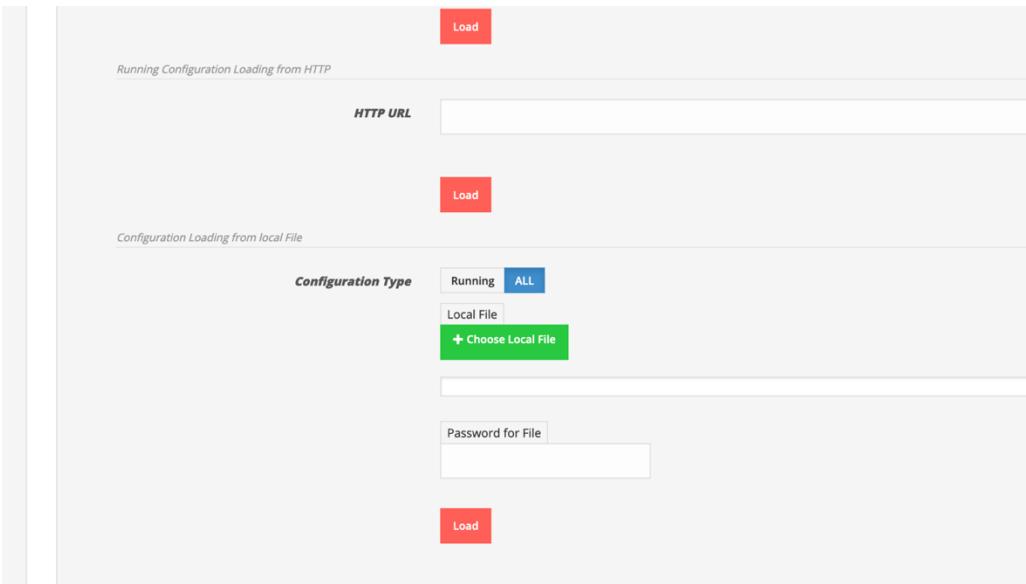
6.1.13 Thiết bị Array Network

Login vào thiết bị.

Truy cập vào System-->Config Management. Chuyển sang Tab Load:



Kéo xuống phía dưới, chọn trong phần Configuration Type là All. Chọn Local File:



Truy xuất đến nơi chứa file Backup để khôi phục lại hệ thống, thiết bị sẽ khởi động lại.

6.2 Hướng dẫn vận hành các máy chủ ảo

6.2.1 Thông tin truy cập vào các thiết bị bên trong VM ESX:

Tên Thiết bị	Địa chỉ truy cập	Tài khoản sinh viên	Vlan	HTTP S	SSH	RDP
VM ESXi	192.168.1.249	student/P@ssword@123	10	x	x	
	172.16.4.243	student/P@ssword@123	4	x	x	
	172.16.5.243	student/P@ssword@123	5	x	x	
DVWA-Vlan5	172.16.5.241		5	http		
FortiSIEM	172.16.4.250		4	x	x	
FortiClient EMS	172.16.4.246	student/fortinet@123	4	x		x
DVWA-241	172.16.4.241		4	http	x	
DVWA-238	172.16.4.238		4	http	x	
DNS	172.16.4.242		4			x
Mail-Centos	172.16.4.239		4	x	x	
Win10	172.16.4.71		4			x

Lưu ý 1 : Những địa chỉ có

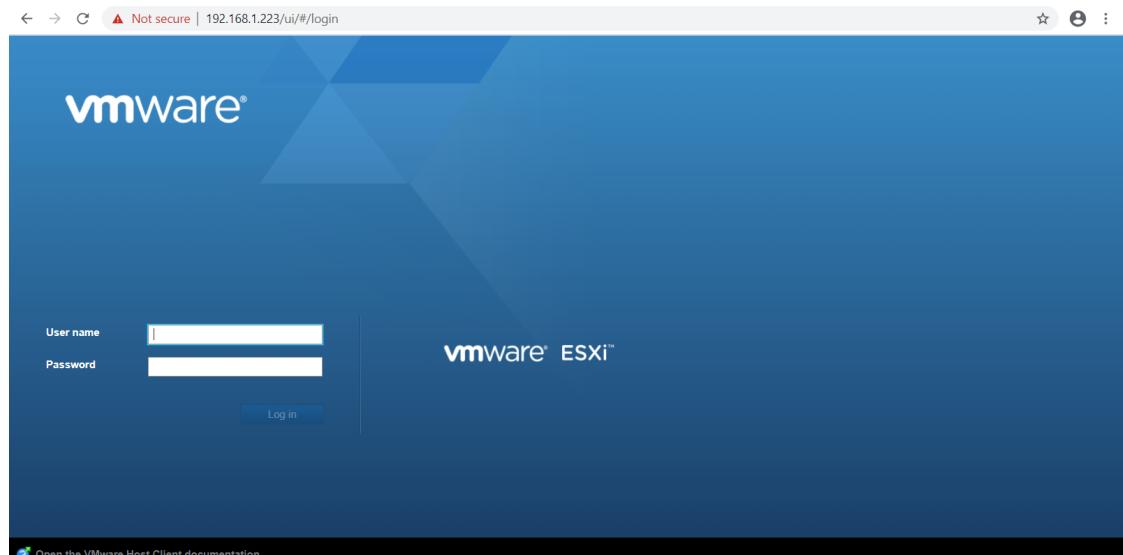
- **HTTPS** truy cập bằng trình duyệt web ! <https://xxx.xxx.xxx.xx:xxxx> (xxxx port kết nối nếu có)
- **SSH** sử dụng putty
- **RDP** sử dụng remote desktop

Lưu ý 2:

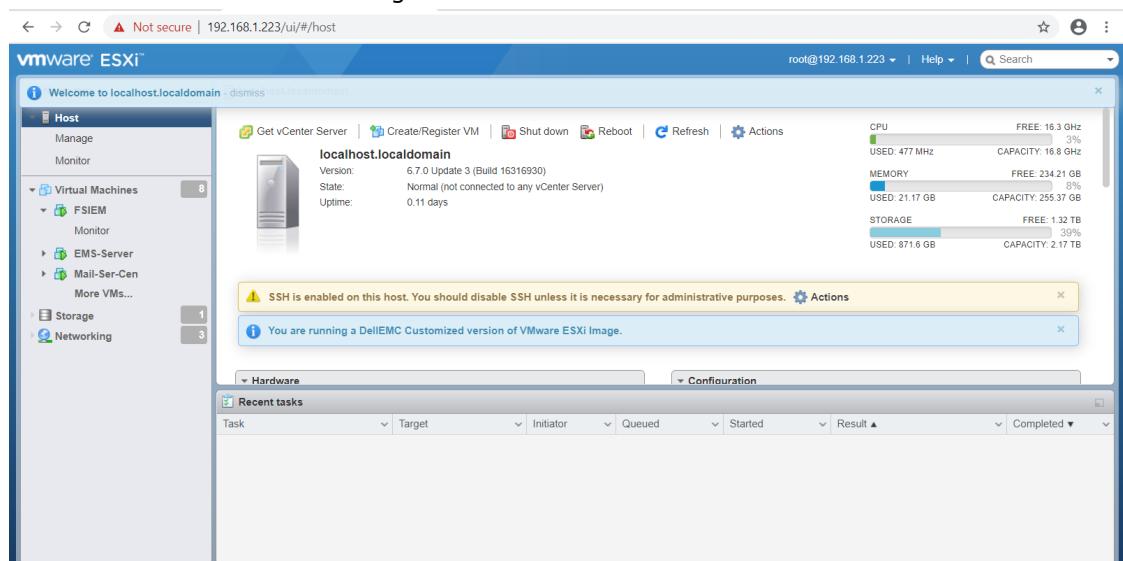
- Đảm bảo các server ảo bên trong được shutdown trước khi tắt điện.
- Khi shutdown các thiết bị bằng tay sẽ phải khởi động lại bằng tay.
- Các Server đã bật sẵn chế độ autostart khi có sự cố.

6.2.2 Hướng dẫn sử dụng VM ESXi

Đăng nhập vào thiết bị VM ESXi

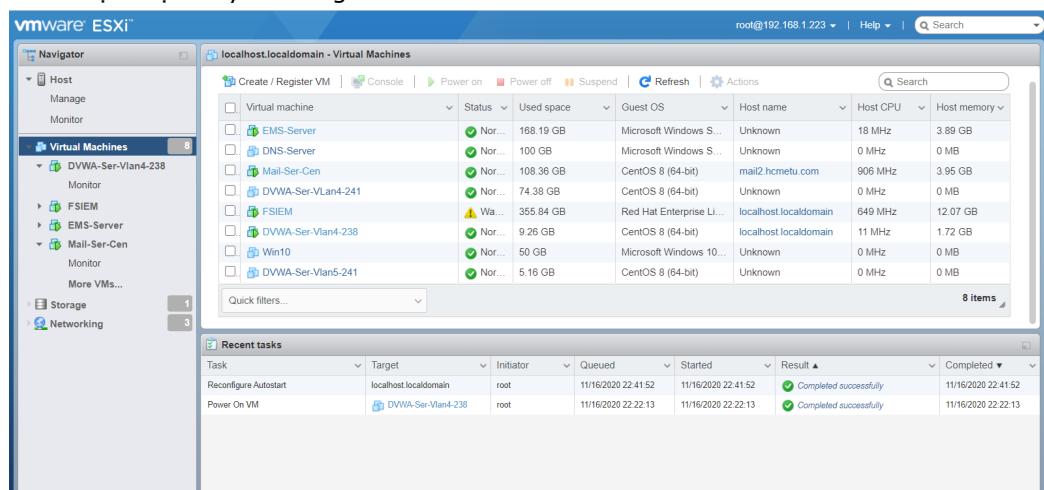


Dashboard Host: chứa các thông tin về VM EXSi

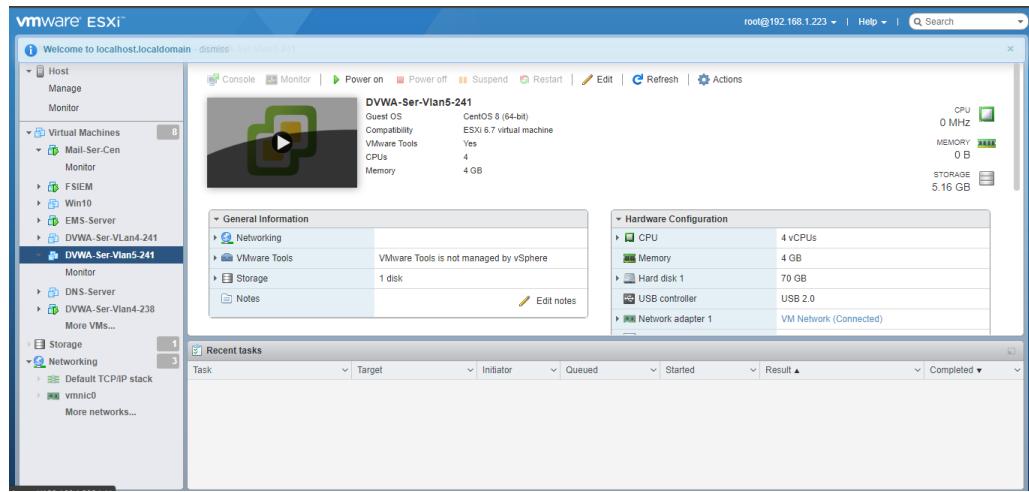


Khởi động các máy ảo bên trong VMware

--> chọn một máy ảo đang offline

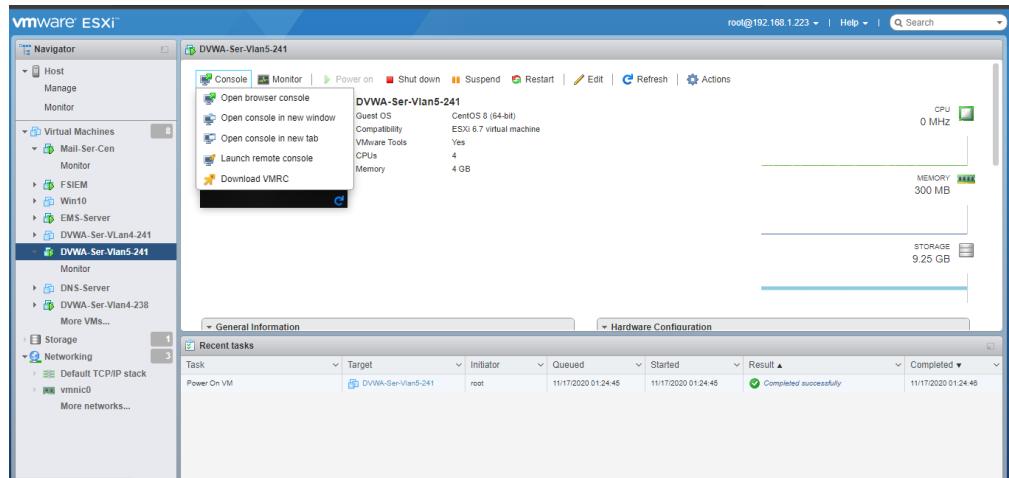


Sau khi vào giao diện quản lý máy ảo! Power on



Mở màn hình máy ảo

Click console ! open console in new window để mở màn hình máy ảo



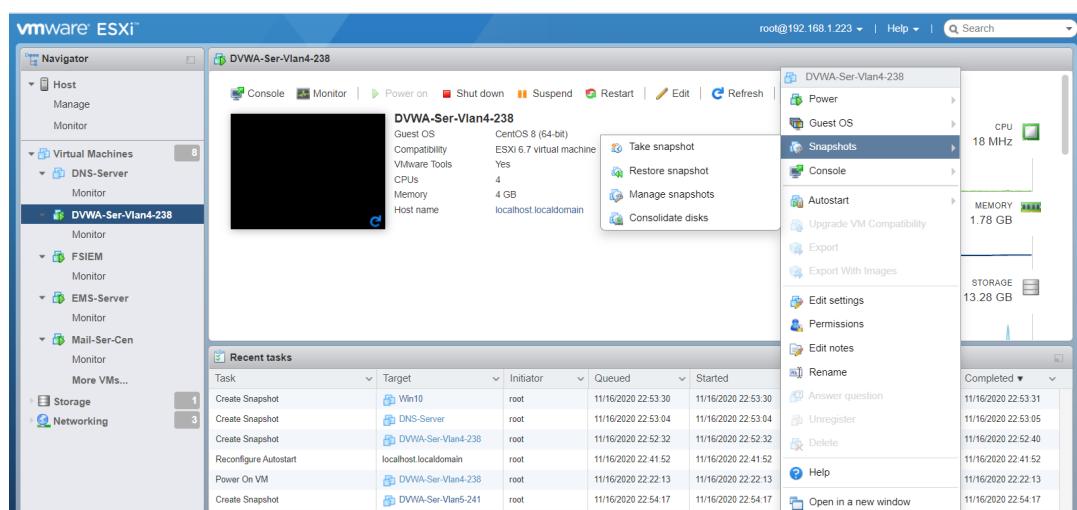
Lưu ý: Tránh sử dụng nút shutdown trực tiếp trên VM trừ trường hợp server bị treo.

Shutdown đúng quy trình.

Snapshot

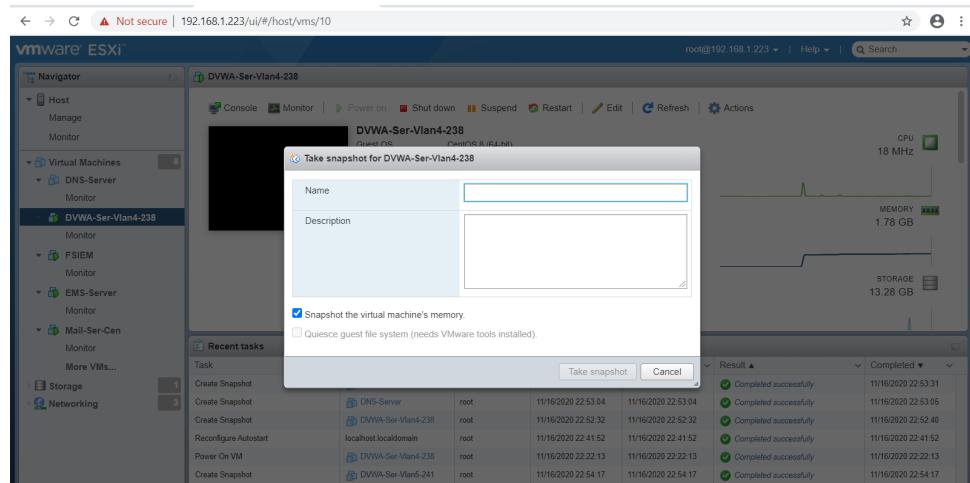
Các máy ảo tránh trường hợp các Server bên trong bị lỗi. Khi lỗi chúng ta có thể restore các bản snapshot trước đó.

Chọn máy ảo ! Action ! Snapshot

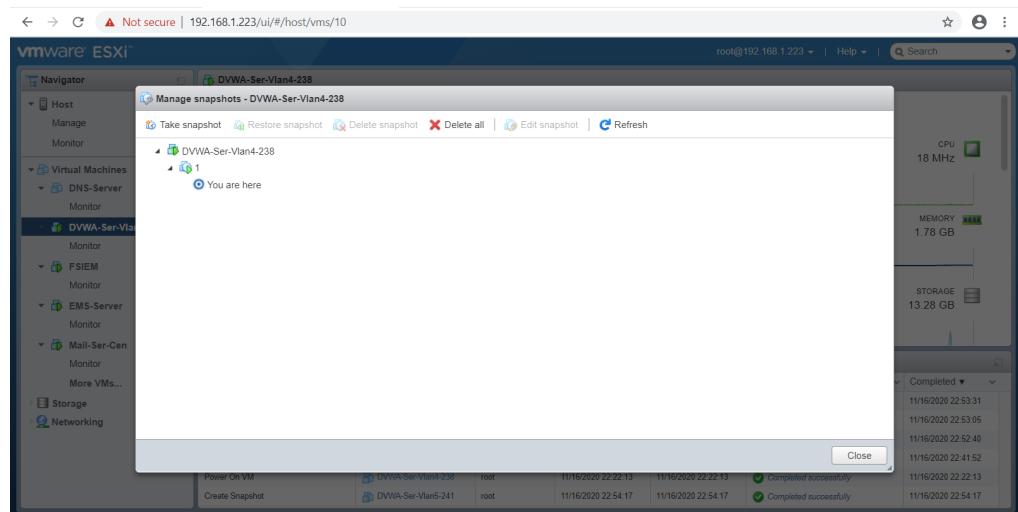


Đặt tên cho bản snapshot của các máy ảo

! Take snapshot

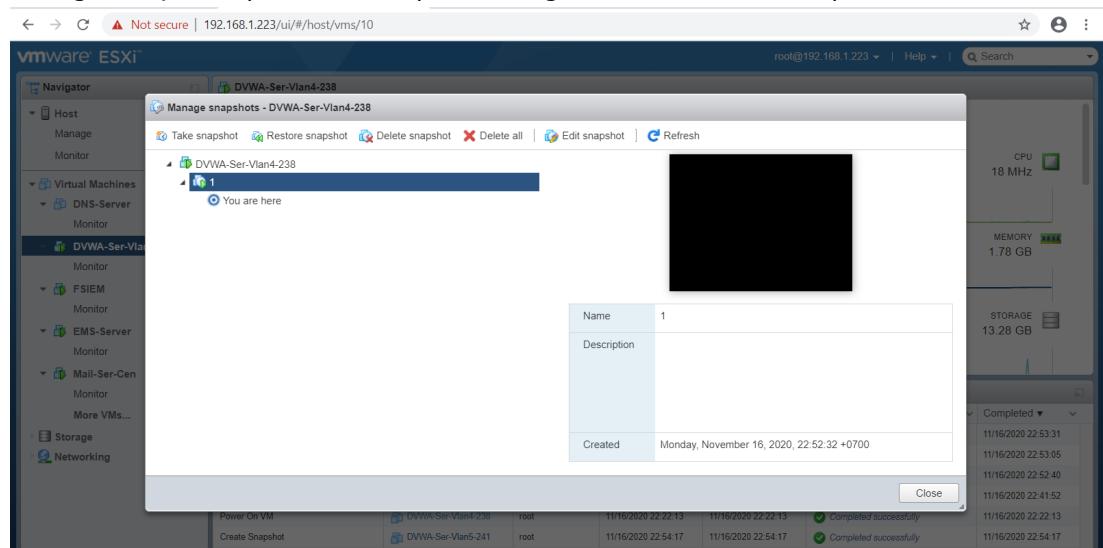


Sau snapshot được thì truy cập vào Action ! Snapshot ! Manage Snapshots
Ở đây chúng ta có thể thấy các phiên bản snapshot trước đó.



Restore snapshot

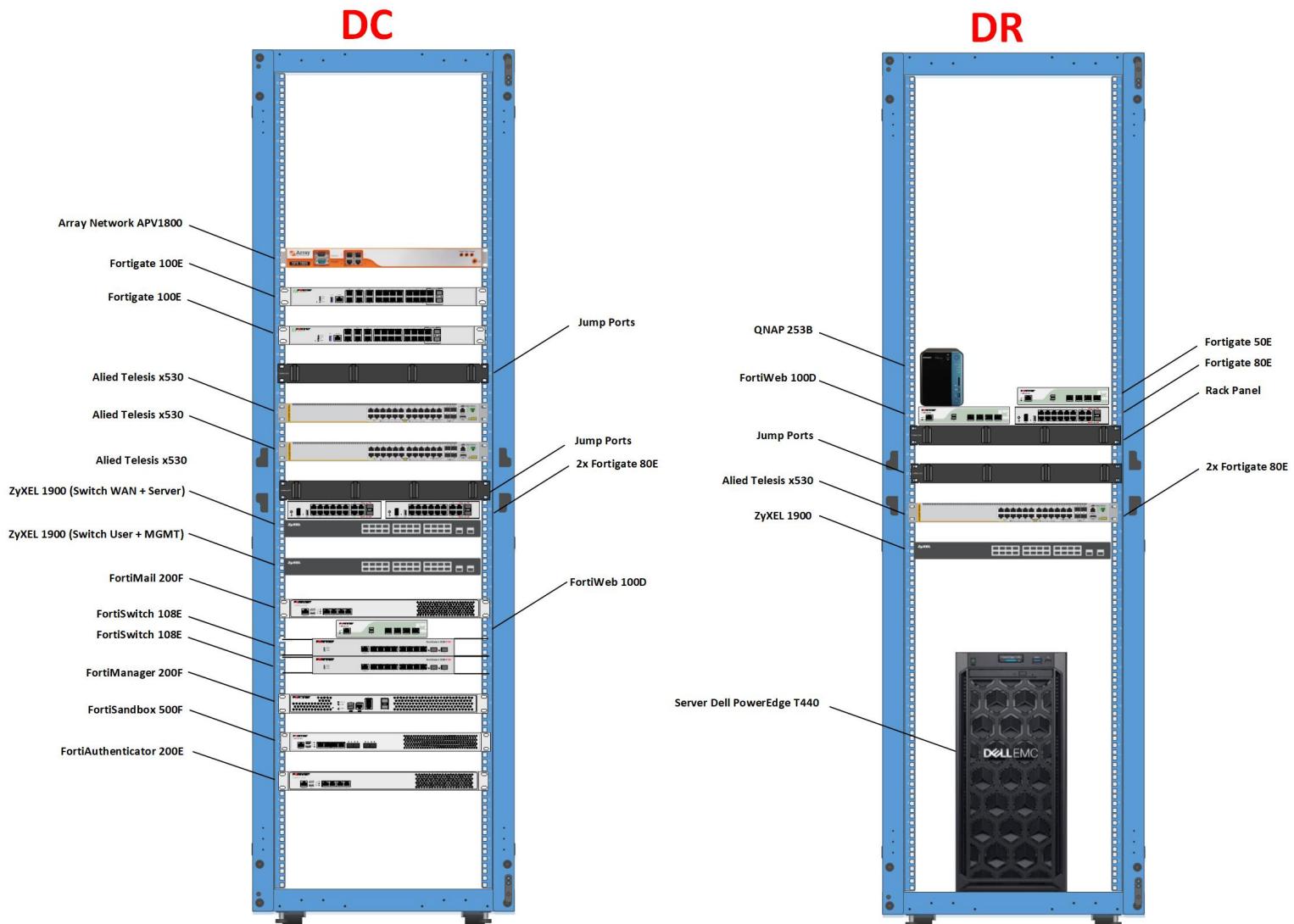
Chúng ta chọn vào phiên bản snapshot mong muốn ! Restore Snapshot



7 Sơ đồ bố trí Rack

7.1 Nguyên lý

Sơ đồ bố trí vật lý các thiết bị vào 2 Tủ Rack 42U cho DC và DR, các thành phần và vị trí như sau:



7.2 Ảnh thực tế

Hình ảnh 2 Tủ DC-DR



Tủ DC



Tủ DR

