HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

_____&*&_____

LÊ NGỌC AN

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT MÁY CHỦ ẢO TRONG HỆ THỐNG ẢO HÓA VÀ ỨNG DỤNG TẠI VIỆN KHOA HỌC CÔNG NGHỆ SÁNG TẠO VIỆT NAM

LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2021

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

_____&*&_____

LÊ NGỌC AN

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT MÁY CHỦ ẢO TRONG HỆ THỐNG ẢO HÓA VÀ ỨNG DỤNG TẠI VIỆN KHOA HỌC CÔNG NGHỆ SÁNG TẠO VIỆT NAM

CHUYÊN NGÀNH : HỆ THỐNG THÔNG TIN

MÃ SỐ : 8.48.01.04

LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. TRẦN QUANG ANH

HÀ NỘI – 2021

LỜI CAM ĐOAN

Tôi cam đoan đề tài: ***"Nghiên cứu giải pháp bảo mật máy chủ ảo trong hệ thống ảo hóa và ứng dụng tại Viện Khoa học công nghệ sáng tạo Việt Nam"*** là công trình nghiên cứu của riêng tôi dưới hướng dẫn của PGS.TS. Trần Quang Anh.

Những khảo sát, phân tích, kết quả trong luận văn này đều là của tác giả, số liệu nêu ra là trung thực và chưa từng được công bố trong bất kỳ công trình nào khác.

Hà Nội, ngày….. tháng…..năm 2021

Tác giả

Lê Ngọc An

LỜI CẢM ƠN

Lời đầu tiên cho tôi xin gửi lời cảm ơn chân thành đến các thầy, cô giáo của Học viện Công nghệ Bưu chính viễn thông đã tận tình chỉ bảo, hướng dẫn, giúp đỡ tôi trong suốt quá trình thực hiện luận văn này.

Tôi xin gửi lời cảm ơn chân thành đặc biệt tới thầy hướng dẫn khoa học PGS.TS. Trần Quang Anh, tận tình chỉ bảo và hướng dẫn, đưa ra định hướng đúng đắn giúp em hoàn thành được luận văn này.

Xin trân trọng cảm ơn các cảm ơn tập thể lớp Cao học hệ thống thông tin khoá 2019-2021 đợt 2, đã đồng hành, khích lệ và chia sẻ trong suốt quá trình học tập và làm luận văn.

Trong quá trình thực hiện luận văn, mặc dù bản thân đã cố gắng, chủ động sưu tầm tài liệu, củng cố kiến thức… tuy nhiên khó có thể tránh khỏi những thiếu sót, hạn chế. Rất mong nhận được sự chỉ dạy, góp ý của các thầy, cô giáo và các bạn cùng lớp để luận văn được hoàn thiện hơn nữa và có tính ứng dụng cao hơn trong thực tiễn.

Xin trân trọng cảm ơn!

Hà Nội, ngày.....tháng..... năm 2021

Học viên

Lê Ngọc An

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Tiếng Việt
AI	Artificial Intelligence	Trí tuệ nhân tạo
CNTT	Information Technology	Công nghệ thông tin
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập
LAN	Local Area Network	Mạng lưới khu vực địa phương
VPN	Virtual Private Network	Mạng riêng ảo

DANH MỤC CÁC HÌNH

MỞ ĐẦU

1. Lý do chọn đề tài

Trong thời kỳ cách mạng công nghiệp 4.0, công nghệ Ảo hóa được phát triển như vũ bão và nổi lên về tính tiết kiệm, cơ động, tiện lợi. Công nghệ Ảo hóa được tạo ra để giao tiếp trung gian giữa hệ thống máy chủ vật lý và phần mềm chạy trên nó, cho phép một máy vật lý có thể tạo thành nhiều máy ảo logic và độc lập. Một máy chủ ảo tương ứng một hệ thống có hệ điều hành chạy riêng và các ứng dụng chạy độc lập.

Giải pháp sử dụng công nghệ Ảo hóa sẽ giải quyết vấn đề chi phí và hiệu suất hoạt động của máy chủ bằng việc giảm chi phí hạ tầng phần cứng và vận hành, sử dụng tối ưu nguồn tài nguyên. Thông qua hạ tầng Ảo hóa triển khai các máy chủ nhanh hơn, dễ dàng, đơn giản hóa việc quản lý hạ tầng bằng cách quản lý tập trung và tự động hóa chu trình làm việc.

Tiện lợi là vậy nhưng thách thức về an ninh mạng và bảo mật cũng được tăng lên với hàng loạt vụ tấn công nhằm vào mạng nội bộ có kết nối Internet của các cơ quan nhà nước và doanh nghiệp. Khi dữ liệu quan trọng bị đánh cắp có thể dẫn đến những tổn thất vô cùng nghiêm trọng, gây nguy hại đến doanh nghiệp, tập đoàn, nhà nước…

Các vụ tấn công nhằm vào các máy tính có mặt trên môi trường mạng Internet, các hạ tầng Ảo hóa, các dịch vụ đang hoạt động, lớn như Google, Apple, IBM, nhiều trường học, cơ quan nhà nước, ngân hàng, … Rất nhiều vụ tấn công với quy mô khổng lồ có tới hàng chục nghìn, trăm nghìn máy tính bị tấn công. Hơn nữa những con số này chỉ là phần nổi, nhiều cuộc tấn công không được công bố hoặc thông báo vì nhiều lý do, trong đó có thể đến nỗi lo mất uy tín hoặc nhiều tình huống quản trị viên hệ thống không hề hay biết những vụ tấn công nhằm vào hệ thống của họ.

Những vụ tấn công tăng lên nhanh chóng, cộng với độ chuyên nghiệp của Hacker cũng được tăng lên. Ở Việt Nam năm các hệ thống mạng và Website bị tấn công theo chiều hướng gia tăng: 2016 hãng hàng không Vietnam Airlines bị tấn

công, Hacker lấy cắp hơn 400.000 dữ liệu khách hàng. Theo thống kê của Trung tâm Ứng cứu sự cố máy tính Việt Nam (VNCERT) đã có hơn 9.300 vụ tấn công mạng nhắm vào các Website của Việt Nam trong năm 2018. So với năm 2017 với 9.964 sự cố tấn công thì các cuộc tấn công mạng đã có xu hướng giảm đi nhưng giảm không đáng kể. Theo báo cáo an ninh website mới nhất được thực hiện bởi CyStack, có hơn 560.000 vụ tấn công vào các website trên toàn cầu trong năm 2019. Việt Nam xếp thứ 11 trên toàn cầu với 9.300 website bị xâm phạm. Trong tháng 5/2020, Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Bộ TT&TT đã ghi nhận được 439 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam.

Từ nhu cầu phát triển công nghệ Ảo hóa cho hạ tầng mạng, máy chủ và dịch vụ, đòi hỏi các hệ thống kết nối vào mạng Internet phải đảm bảo an toàn thông tin trong quá trình kết nối. Bởi vậy, học viên đã lựa chọn đề tài: **"Nghiên cứu giải pháp bảo mật máy chủ ảo trong hệ thống ảo hóa và ứng dụng tại Viện Khoa học công nghệ sáng tạo Việt Nam"** cho luận văn tốt nghiệp trình độ đào tạo thạc sĩ.

2. Tổng quan nội dung nghiên cứu

Công nghệ Ảo hóa (Virtualization): ra đời vào những năng 1960s trong các máy tính Mainframe, các thiết bị phần cứng, máy chủ, hạ tầng mạng, hệ thống lưu trữ… và hơn thế nữa. Nhưng để xét sự phát triển vượt bậc và bùng nổ thì từ năm 2000 với sự tham gia của các hãng như VMWare, CITRIX, Microsft…. Tới năm 2010 OpenStack (nguồn mở) ra đời đóng góp vào sự sôi động của của cộng đồng công nghệ Ảo hóa.

Thuật ngữ Ảo hóa (Virtualization) đề cập đến hành động tạo ra phiên bản "Ảo" (chứ không phải thực tế) của phần mềm, phần cứng hay một cái gì đó, bao gồm cả một tập tài nguyên về mạng máy tính… nhưng không hề bị hạn chế.

Các thành phần thông thường của một hệ thống Ảo hóa: Tài nguyên vật lý (máy chủ vật lý, CPU, RAM, ổ đĩa cứng, card mạng…) Nhiệm vụ là chia tài nguyên cấp cho các máy ảo. Tiếp theo là phần mềm Ảo hóa (Hypervisor) sẽ cung cấp truy

cập cho mỗi máy chủ ảo đến tài nguyên của máy chủ vật lý, lập kế hoạch và phân chia tài nguyên vật lý cho các máy chủ ảo, cung cấp giao diện quản lý cho các máy chủ ảo. Kế tiếp là hệ điều hành khách (Guest Operating System) được cài đặt trên một máy chủ ảo, thao tác như ở trên hệ điều hành thông thường. Cuối cùng là máy ảo (Virtual Machine) hoạt động như một máy chủ vật lý thông thường với tài nguyên riêng, giao diện riêng, hệ điều hành riêng, phục vụ nhu cầu độc lập của các dịch vụ như: Website, Email, File, DNS, DHCP….

Trong phần mềm Ảo hóa (Hypervisor) cung cấp công nghệ Ảo hóa về hạ tầng mạng (Virtual Networks), cho phép kết nối giữa Switch vật lý, hạ tầng vật lý từ bên ngoài vào bên trong Switch ảo. Các máy chủ ảo hoạt có dịch vụ chạy (Web, Mail, File…) hoạt động độc lập như các máy chủ vật lý. Trên Switch ảo có thể tách VLAN (Virtual Local Area Network), đặt các hệ thống tường lửa mềm, đặt hệ thống phát hiện xâm nhập, hệ thống chống tấn công (IDS/IPS) giúp chống lại các cuộc tấn công từ bên ngoài vào hệ thống dịch vụ bên trong. Đặc biệt khi xảy ra tấn công, có thể chuyển hệ thống máy chủ ảo sang vùng mới nhanh chóng mà không cần phải rút dây, hoặc ngắt toàn bộ hệ thống. Ngoài ra có thể đặt các hệ thống máy chủ theo dõi, giám sát, truy vết rất thuận tiện trong hạ tầng Ảo hóa.

Khi xây dựng một hệ thống tường lửa dùng để bảo vệ hệ thống máy chủ ảo chúng ta có nhiều giải pháp như sử dụng tường lửa cứng như ASA của Cisco, RSX của Juniper, Checkpoint, Fortigate hoặc của Microsoft như TMG… nhưng chi phí rất đắt tiền vì phải mua cả phần cứng. Các hãng vẫn hỗ trợ hệ điều hành chạy trên máy chủ ảo, chỉ cần cài lên, gán key bản quyền là chạy bình thường, không phải mua thiết bị vật lý, tiết kiệm rất nhiều chi phí.

Những thuận lợi và tiện ích về công nghệ Ảo hóa là vậy nhưng không phải không có khó khăn. Việc khó khăn lớn nhất là sự tiếp cận công nghệ, làm chủ công nghệ, đặc biệt là khó khăn về tối ưu bảo mật cho máy chủ trên nền tảng Ảo hóa. Người quản trị viên phải hiểu từ hạ tầng vật lý, nền tảng công nghệ Ảo hóa, dịch vụ triển khai, cơ chế và chính sách bảo mật, chính sách về con người. Và vấn đề này vẫn được tiếp tục nghiên cứu cả về mặt lý thuyết lẫn triển khai ứng dụng.

3. Mục tiêu nghiên cứu

Mục tiêu nghiên cứu của luận văn là khảo sát các yêu cầu và giải pháp bảo mật máy chủ ảo trong hệ thống Ảo hóa đồng thời đề xuất giải pháp bảo mật máy chủ ảo trong hệ thống Ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam có khả năng triển khai áp dụng trong thực tế.

4. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của luận văn là Ảo hóa và các vấn đề liên quan đến bảo mật máy chủ ảo trong hệ thống Ảo hóa.

Phạm vi nghiên cứu của luận văn là các giải pháp bảo mật máy chủ ảo trong hệ thống Ảo hóa và ứng dụng cho hệ thống máy chủ Ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam.

5. Phương pháp nghiên cứu

- ***Về lý thuyết***: Thu thập thông tin từ tài liệu, khảo sát, phân tích thực tế và thông tin có liên quan đến bảo mật máy chủ ảo trong hệ thống Ảo hóa.

- ***Về thực nghiệm***: Khảo sát thực tế tại Viện Khoa học công nghệ sáng tạo Việt Nam và đề xuất các giải pháp bảo mật máy chủ ảo trong hệ thống Ảo hóa của Viện Khoa học công nghệ sáng tạo Việt Nam phù hợp.

6. Bố cục luận văn

Luận văn được trình bày trong 3 chương:

Chương 1 của luận văn sẽ nghiên cứu, khảo sát tổng quan về công nghệ Ảo hóa và các các yêu cầu bảo mật đối với máy chủ ảo chạy trên nền tảng Ảo hóa.

Chương 2 của luận văn tập trung nghiên cứu các giải pháp bảo mật đối với máy chủ ảo chạy trên nền tảng Ảo hóa.

Chương 3 của luận văn sẽ khảo sát về hệ thống Ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam (đã có hay chưa có) và đề xuất ứng dụng, xây dựng cũng như đưa các giải pháp đã nghiên cứu trong chương 2 cho hệ thống máy chủ ảo tại Viện Khoa học công nghệ sáng tạo Việt Nam.

Chương 1. TỔNG QUAN CÔNG NGHỆ ẢO HÓA VÀ YÊU CẦU BẢO MẬT MÁY CHỦ ẢO

Chương 1 của luận văn sẽ nghiên cứu, khảo sát tổng quan về công nghệ Ảo hóa và các các yêu cầu bảo mật đối với máy chủ ảo chạy trên nền tảng Ảo hóa. Nội dung trình bày trong chương 1 bao gồm như sau:

1.1 Tổng quan về công nghệ Ảo hóa và các vấn đề liên quan

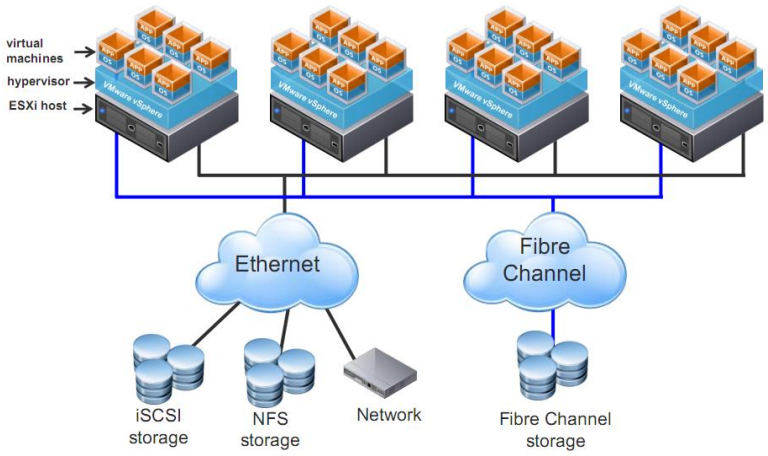
1.1.1 Giới thiệu tổng quang về các công nghệ ảo hóa

1.1.1.1 Giới thiệu chung

Ảo hóa có tên tiếng anh thường gọi là "Virtualization": ra đời vào khoảng 1960s trong các máy tính Mainframe.

Trong lĩnh vực điện toán, thuật ngữ "Virtualization" đề cập đến hành động tạo ra phiên bản "Ảo" của phần mềm, phần cứng hay một cái gì đó, bao gồm cả một tập tài nguyên về mạng máy tính… nhưng không hề bị hạn chế.

Công nghệ tạo ra lớp trung gian giữa hệ thống phần mềm và phần cứng chạy trên nó được gọi là Ảo hóa. Công nghệ ảo hóa cho phép gộp nhiều máy chủ vật lý ở dạng đơn lẻ thành nhiều máy chủ Logic, đồng thời các máy chủ Logic này có thể chạy các ứng dụng trên các hệ điều hành độc lập.



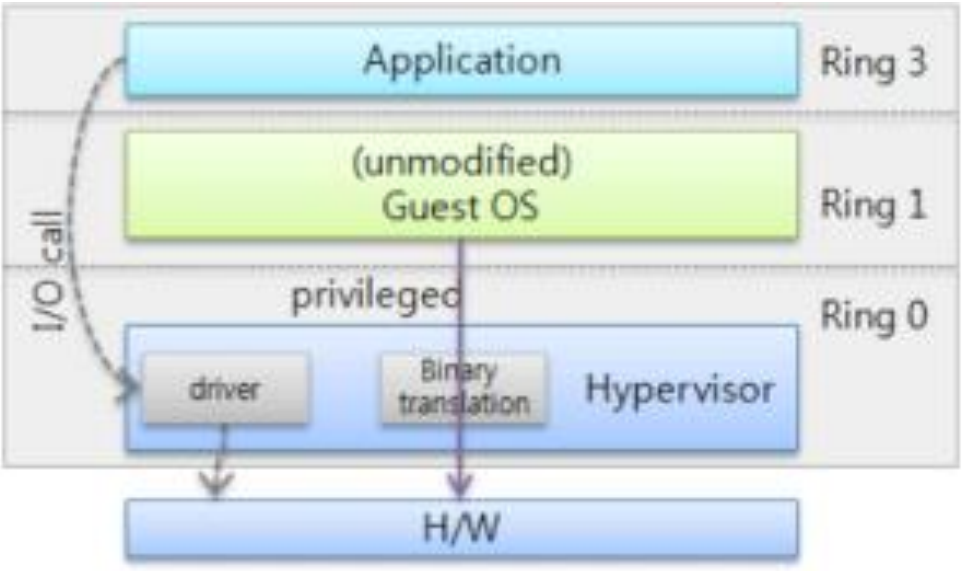
Hình 1.1: Giới thiệu mô hình hệ thống ảo hóa phổ biến [8]

Tại sao cần ảo hóa: Giảm thiểu chi phí bảo dưỡng, tương thích với nhiều ứng dụng, hệ điều hành đồng thời, tập trung cho kiểm soát và quản trị, dễ dàng trong sao lưu và khôi phục, khai thác nhiều hơn về công suất hoạt động phần cứng, chuyển đổi các máy ảo kể cả khi đang hoạt động, nâng cao độ sẵn sàng cho hệ thống và là bước đệm để thực hiện "Điện toán đám mây".

1.1.1.2 Giới thiệu một số dạng ảo hóa máy chủ

Ảo hóa máy chủ thường được xây dựng theo 3 dạng: ảo hóa toàn phần, ảo hóa một phần và ảo hóa hệ điều hành.

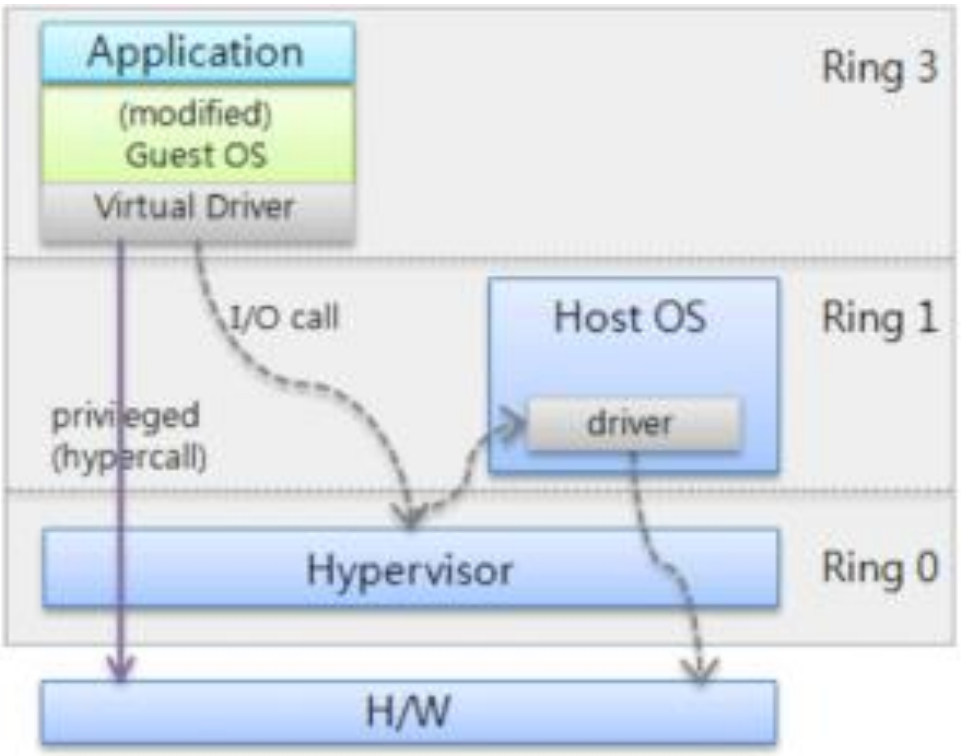
- Full Virtualization: tiếng việt gọi là Ảo hóa toàn phần, công nghệ ảo hóa này tạo ra một máy chủ thật với đầy đủ tất cả các tính năng bao gồm input/output, operations, interrupts, memory access … Các máy chủ ảo sẽ được chạy những hệ điều hành riêng và được cấp riêng CPU, RAM, dung lượng lưu trữ và băng thông mạng. Các máy ảo hoàn toàn nằm độc lập với lớp Hardware và sẽ giao tiếp với Hypervisor, nên tốc độ sẽ bị chậm hơn vì phải qua Binary translation. Các bản nguồn mở hỗ trợ như: KVM, KQEMU, VIRTUABOX. Bản thương mại: VMware, Microsoft (Hyper-V).



Hình 1.2: Cấu trúc liên kết các tầng của ảo hóa toàn phần [8]

- Para – Virtualization: tiếng việt gọi là ảo hóa một phần, kỹ thuật này vẫn được điều khiển bằng một Hypervisor, các máy chủ ảo khi làm việc sẽ tương tác

trực tiếp xuống hạ tầng phần cứng mà không phải tương qua qua môi trường Hypervisor, qua đó sẽ tạo ra tốc độ xử lý nhanh hơn. Nhưng nhược điểm sẽ là các máy chủ ảo sẽ khó cài đặt và cấu hình hơn. Một số hệ điều hành xây dựng theo kiểu Para – Virtualization Xen Server, VMWare Server và Hyper–V của Microsoft. Trình điều khiển hypervisor sử dụng một kernel đơn để quản lý các máy chủ ảo và cho phép chúng chạy đồng thời trên máy chủ vật lý ban đầu.



Hình 1.3: Cấu trúc liên kết các tầng của ảo hóa một phần [8]

- OS level Virtualization: Tiếng việt gọi là Ảo hóa hệ điều hành, là phương pháp ảo hóa mới cho phép nhân của hệ điều hành hỗ trợ nhiều instances được cách ly dựa trên hệ điều hành có sẵn cho nhiều người dung khác nhau. Việc bảo trì nhanh nên mọi người hay dùng, nhất là trong lĩnh vực Hosting. OpenVZ, Virtuozzo, Linux – VServer, Solaris Zones, và FreeBSD Jails hỗ trợ loại ảo hóa này. Loại ảo hóa này chỉ tồn tại trên hệ điều hành Linux, ảo hóa hệ điều hành rất hữu ích cho các công ty máy chủ Web.

1.1.1.3 Môi trường ảo hóa

Môi trường ảo hóa trên nền tảng Window: công nghệ ảo hóa thế hệ mới của

Microsoft tạo ra có tên là Hyper – V, phục vụ khai thác phần cứng máy chủ 64 bit thế hệ mới, linh hoạt, mạnh mẽ và có thể triển khai được nhiều cấp độ khác nhau.

Các máy ảo do Hyper-V tạo ra sẽ rất thuận tiện trong điều chỉnh cấu hình, có thể mở rộng dung lượng lớn, tùy chỉnh CPU đa nhân. Môi trường Hypervisor hỗ trợ thân thiện bằng giao diện đồ họa giúp quản trị viên có thể tùy chỉnh và cấu hình thuận tiện các tính năng khác. Các máy ảo sẽ tương tác với phần cứng qua môi trường Hypervisor và áp dụng theo Full Virtualization.

Môi trường ảo hóa trên Linux: Kernel – based Virtual Machine (KVM) là một trình quản lý ảo hóa phần cứng được xây dựng trên nền nhân Linux. KVM là giải pháp ảo hóa toàn phần dành cho những phần cứng trên nền tảng 32 bit và 64 bit của VT –X hay AMD.

Sử dụng KVM, một máy chủ vật lý có thể chạy nhiều máy ảo trên đó với những hệ điều hành khác nhau như GNU/Linux, Window hay bất kỳ một hệ điều hành nào. Mỗi máy ảo có những phần cứng ảo riêng như thẻ mạng, đĩa cứng, hay thẻ đồ họa.

Phần cứng hỗ trợ KVM nguyên bản hỗ trợ các bộ xử lý 32 bit như S/390, PowerPC, IA – 64. KVM yêu cầu bộ xử lý máy chủ ảo hỗ trợ ảo hóa VT – x cho bộ xử lý của Intel và AMD – V cho bộ xử lý AMD.

Môi trường ảo hóa trên nền tảng VMware vSphere: VMWare tạo ra 2 phiên bản cho môi trường Server và môi trường Client. Trong phần này chỉ xét tới môi trường Server gọi là VMware vSphere. Khi triển khai hệ thống nó sẽ tạo ra một môi trường Hypervisor để quản lý và phân chia tài nguyên cho các máy ảo. Các máy ảo chỉ bị môi trường Hypervisor quản lý còn khi hoạt động sẽ tương tác thẳng xuống tài nguyên vật lý của máy chủ mà không phải đưa qua môi trường Hypervisor, giúp tận dụng tối đa hiệu suất hoạt động của máy chủ vật lý và các máy ảo, đồng thời cũng thuận tiện quản lý hơn.

Môi trường ảo hóa trên nền tảng OpenStack: OpenStack là phần mềm mã nguồn mở, dùng để triển khai điện toán đám mây, bao gồm đám mây công cộng và đám mây riêng. OpenStack được thiết kế theo lối module, mỗi phần đảm nhận

những công việc khác nhau của hệ thống quản lý ảo hóa. OpenStack không phải là một dự án đơn lẻ mà là một nhóm các dự án nguồn mở tập hợp nhiều công nghệ ảo hóa, hỗ trợ cho việc xây dựng hạ tầng đám mây công cộng và đám mây riêng hoàn chỉnh.

OpenStack bao gồm một số thành phần chính: Dashboard, Compute, Object storage, Image storage, Block storage, Network, Identity. Mỗi thành phần có nhiều plugin bên trong thực hiện những tác vụ chuyên biệt, tất cả các thành phần đều có một plugin cung cấp API để giao tiếp với nhau và giao tiếp với người dùng.

OpenStack Glance quản lý các ảnh đĩa ảo. Glance hỗ trợ các ảnh Raw, VirtualBox (VDI), Qemu (qcow2) và VMWare (vmdk, ovf). Người dùng có thể thực hiện: cập nhật thêm các ảnh đĩa ảo, cấu hình và điều khiển việc truy cập vào chúng.

1.1.2 Các mối đe dọa và phương thức tấn công hệ thống ảo hóa

1.1.2.1 Những mối đe dọa tới an toàn thông tin

Giới thiệu về kiểu đe dọa không có cấu trúc: thường là những hành vi xâm nhập hệ thống ảo hóa trái phép một cách đơn lẻ, không có tổ chức. Trên Internet có rất nhiều công cụ có thể hack và rất nhiều script có sẵn. Chỉ cần ai muốn tìm hiểu có thể tải chúng về và sử dụng thử để nghiên cứu trên mạng nội bộ của công ty. Rất nhiều người lại thích với việc tấn công và xâm nhập vào hệ thống ảo hóa và thử thách các hành động vượt tường lửa đi ra khỏi tầm bảo vệ. Đa phần tấn công không có cấu trúc đều được gây ra bởi Script Kiddies hay những người có trình độ thấp hoặc vừa phải vừa phải. Những cuộc tấn công đó thường vì sở thích cá nhân, nhưng cũng có nhiều cuộc tấn công có ý đồ xấu để lấy cắp thông tin. Các trường hợp đó sẽ có ảnh hưởng nghiêm trọng đến hệ thống ảo hóa và các chủ thể sở hữu mạng. Nhiều lúc, chỉ cần có một đoạn mã độc là có thể phá hủy chức năng của mạng nội bộ và hệ thống máy chủ đang chạy trên các nền tảng ảo hóa.

Giới thiệu về kiểu đe dọa có cấu trúc: là những cách thức tấn công hoặc xâm nhập hệ thống mạng trái phép hoặc hệ thống máy chủ ảo, có động cơ và kỹ thuật cao. Hacker tấn công theo kiểu này hoạt động độc lập hoặc theo từng nhóm. Những

kẻ tấn công này thường có kỹ năng phát triển ứng dụng và sử dụng các kỹ thuật phức tạp nhằm xâm nhập vào mục tiêu có chủ đích. Những động cơ của các hình thức tấn công này thì có rất nhiều mục đích. Chẳng hạn như có thể vì tiền hoặc hoạt động chính trị đôi khi là tức giận hay báo thù. Các nhóm tội phạm, các đối tác, đối thủ cạnh tranh hay các tổ chức sắc tộc thuê các hacker để thực hiện các cuộc tấn công, kiểm soát dạng structured threat. Những cuộc tấn công vào hệ thống thường có nhiều mục đích từ trước, qua đó có thể lấy được mã nguồn của những đối thủ cạnh tranh với nhau.

Những động cơ đó có là gì, thì các cuộc tấn công như vậy rất có thể gây hậu quả nghiêm trọng, có thể gây nên sự phá hủy cho toàn hệ thống mạng và hệ thống ảo hóa của doanh nghiệp hoặc các tổ chức.

Những mối đe dọa từ bên ngoài: là những cuộc tấn công được tạo ra khi Hacker không có một quyền nào kiểm soát trong hệ thống. Người dùng có thể bị tấn công trên toàn thế giới thông qua mạng Internet. Những mối đe dọa từ bên ngoài này thường là mối đe dọa nguy hiểm, các chủ doan nghiệp sở hữu mạng LAN và hệ thống ảo hóa thường phải bỏ rất nhiều tiền và thời gian để bảo vệ hệ thống.

Những mối đe dọa từ bên trong hệ thống: là kiểu tấn công được thực hiện từ một cá nhân hoặc một tổ chức có một số quyền truy cập vào hệ thống mạng nội bộ của công ty, hệ thống ảo hóa. Những cách tấn công này thường từ bên trong, được thực hiện từ một vị trí tin cậy trong mạng nội bộ, rất khó phòng chống bởi đôi khi chính là các nhân viên truy cập mạng rồi tấn công. Nhưng nếu có hệ thống giám sát và phân tích sẽ rất dễ bắt được các đối tượng này.

1.1.2.2 Những cách thức tấn công hệ thống ảo hóa

Cách thức lấy cắp thông tin bằng kiểu tấn công Packet Sniffers

Chương trình ứng dụng này tạo ra dùng để bắt giữ các các gói tin lưu chuyển trên hệ thống mạng, hệ thống mạng ảo hóa hoặc trên một miền mạng riêng. Kiểu Sniffer thường được dùng phân tích lưu lượng (traffic). Nếu một số ứng dụng không mã hóa mà gửi dữ liệu dưới dạng clear text (telnet, POP3, FTP, SMTP,...) thì phần

mềm sniffer cũng là một công cụ giúp cho hacker bắt được các thông tin nhạy cảm như là username, password, từ đó có thể đăng nhập vào các hệ thống máy chủ ảo.

Cách thức lấy cắp mật khẩu bằng Password attack

Hacker thường tấn công lấy cắp mật khẩu bằng các phương pháp như: kiểu brute-force attack, hay chương trình Trojan Horse, hoặc IP spoofing, và packet sniffer. Đối với kiểu dùng packet sniffer hoặc IP spoofing có thể lấy được tài khoản và mật khẩu (user account và password), như các Hacker lại thường sử dụng kiểu brute-force để lấy tài khoản và mật khẩu hơn. Cách thức tấn công brute-force được thực hiện bằng phương pháp dùng một chương trình chạy trên hệ thống mạng, sau đó cố gắng login vào các phần chia sẻ tài nguyên trên máy chủ ảo.

Phương pháp tấn công thông qua Mail Relay

Nếu máy chủ ảo chạy dịch vụ Email không cấu hình theo chuẩn hoặc tài khoản và mật khẩu của người dùng sử dụng mail bị lộ. Các Hacker thường lợi dụng máy chủ ảo chạy dịch vụ Email để gửi rất nhiều mail cùng lúc gây ngập băng thông mạng, và phá hoại các hệ thống email khác. Đặc biệt kiểu gắn thêm những đoạn script trong mail, các hacker có thể gây ra các cuộc tấn công Spam đồng thời với khả năng tấn công gián tiếp đến các máy chủ chứa Database nội bộ của công ty hoặc các cuộc tấn công DoS vào một mục tiêu nào đó có chủ đích.

Cách thức tấn công tầng ứng dụng

Hacker tấn công vào tầng ứng dụng được thực hiện bằng rất nhiều cách khác nhau. Những cách thông dụng nhất thường là tấn công vào các điểm yếu của các phần mềm như HTTP, hoặc FTP. Các nguyên nhân chủ yếu của các cuộc tấn công tầng ứng dụng là chúng sử dụng các cổng được mở bởi tưởng lửa của hệ thống . Ví dụ Hacker thường tấn công dịch vụ Web server bằng cách sử dụng một số phần mềm quét port 80 sau đó tấn công hoặc dịch vụ mail server qua port 25.

Cách thức tấn công bằng Virus và phần mềm Trojan Horse

Những nguy hiểm của các máy chủ ảo, máy workstation và người dùng đầu cuối là những tấn công virus và Trojan (thường gọi là Trojan horse). Phần mềm Virus thường là có hại, chúng được đính kèm vào các chương trình thực thi để thực

hiện một cách thức phá hại nào đó. Còn phần mềm Trojan horse thì hoạt động theo kiểu gián điệp, nghe lén và lấy cắp thông tin.

1.2 Ứng dụng công nghệ Ảo hóa

1.2.1 Chạy các phần mềm và các dịch vụ cũ

Khi máy chủ của doanh nghiệp đã được nâng cấp lên hệ điều hành mới nhất nhưng lại có thêm những chương trình, phần mềm không tương thích với hệ điều hành mới mà chỉ có thể chạy được trên hệ điều hành cũ. Việc tạo ra máy chủ ảo với hệ điều hành cũ để chương trình, phần mềm có thể hoạt động được là giải pháp tối ưu nhất.

1.2.2 Kiểm tra dữ liệu nghi nhiễm virus

Máy chủ là trung tâm xử lý các dữ liệu, thông tin của toàn bộ doanh nghiệp. Nếu máy chủ bị nhiễm virut thì toàn bộ các dữ liệu, thông tin của doanh nghiệp đều bị ảnh hưởng. Một môi trường ảo giúp kiểm tra dữ liệu hoàn toàn tách biệt với môi trường hoạt động của máy chủ là giải pháp cần thiết và dịch vụ thuê vps hiện nay được đánh giá cao do hệ thống được các chuyên gia kỹ thuật giám sát, áp dụng các biện pháp bảo vệ tiên tiến nhất

1.2.3 Truy cập website an toàn hơn

Sự phát triển mạnh mẽ của công nghệ thông tin và internet tạo nên những mối nguy cơ tiềm ẩn nhằm gây tác động xấu đến dữ liệu: tấn công, đánh cắp dữ liệu…Để an toàn cho hệ thống máy chủ, doanh nghiệp, người quản trị máy chủ nên truy cập website từ máy chủ ảo

1.2.4 Chạy thử nghiệm phần mềm mới

Môi trường giả lập của máy chủ ảo không chỉ giúp người dùng kiểm tra các dữ liệu nghi nhiễm virut, dùng để truy cập website một cách an toàn mà còn dùng để chạy các phần mềm mới, hay kiểm thử các thiết lập mới.

1.2.5 Chạy 2 điều hành song song

Các chương trình ứng dụng của doanh nghiệp không phải chương trình, phần mềm nào cũng có thể hoạt động được trên hệ điều hành Windows hay Linux. Dùng

máy chủ có nhiều hơn 1 hệ điều hành giúp doanh nghiệp dễ dàng có được các chương trình, phần mềm, ứng dụng phù hợp với nhu cầu sử dụng của doanh nghiệp

1.2.6 Chạy các máy chủ quản lý dịch vụ

Ứng dụng của công nghệ ảo hóa chính là những lợi ích chính mà doanh nghiệp có được khi ảo hóa máy chủ để tạo ra máy chủ ảo. Ngoài ra, doanh nghiệp có thể tạo ra máy chủ ảo để làm máy chủ game, máy chủ mail, Web, DNS, File…

1.3 Các yêu cầu bảo mật chung cho máy chủ ảo trên nền tảng Ảo hóa

1.3.1 Yêu cầu bảo mật về hạ tầng mạng và máy chủ ảo

Khi khai thác hạ tầng ảo hóa hay hạ tầng mạng LAN, đều có những phát sinh nguy cơ về lỗ hổng bảo mật. Thời kì công nghệ phát triển nhanh chóng, các công cụ và kỹ thuật tấn công vào hệ thống mạng cũng càng dễ dàng hơn. Khi các quản trị viên xây dựng và quản lý hệ thống, nếu sắp xếp hoặc cấu hình không đúng cách cũng càng góp phần tạo ra các lỗ hổng. Đặc biệt hệ thống và hạ tầng ảo hóa lại càng phức tạp, người quản trị không kiểm soát tốt sẽ có nhiều lỗi và lỗ hổng kèm theo đằng sau, tạo môi trường thuận tiện cho các hacker tấn công.

Bảo mật hạ tầng máy chủ ảo, hạ tầng ảo hóa, hạ tầng mạng nội bộ của công ty đã trở thành vấn đề hàng đầu trong quản lý vận hành. Khi thiết kế cần ưu tiên một số vấn đề sau: Ứng dụng công nghệ VLAN để tách các Switch ảo trong hạ tầng Ảo hóa (Hypervisor). Tạo ra hệ thống phát hiện xâm nhập và chặn xâm nhập cho máy chủ ảo. Xây dựng hệ thống tường lửa mềm để bảo vệ các máy chủ ảo. Đồng thời phải tuân thủ các yêu cầu:

Đảm bảo tính sẵn sàng của hệ thống mạng: đảm bảo hạ tầng ảo hoát phải hoạt động được 24/7.

Đảm bảo tính bền vững: phải chịu tải và chống lại được các cuộc tấn công nội bộ từ mạng LAN hoặc các cuộc tấn công từ bên ngoài, luôn luôn kiểm soát được hoạt động của các dịch vụ.

Đảm bảo về độ tin cậy: trong khi hệ thống hoạt động, hạ tầng ảo ảo hóa và máy chủ ảo luôn phải được đảm bảo và kiểm soát được việc truy cập của người dùng là hợp pháp, tránh các rủi ro xẩy ra gây mất an toàn.

Khi xây dựng hệ thống ảo hóa và máy chủ ảo ta cần nắm được chu trình bảo mật gồm các giai đoạn: Bảo mật an ninh hạ tần mạng và hạ tầng ảo hóa (Secure); giám sát hạ tầng ảo hóa và các máy chủ hoạt động (Monitor); luôn luôn thực hiện kiểm tra các lỗi và những lỗ hổng phát sin trong hệ thống (Test); luôn luôn phải cải tiến và nâng cấp các chính sách phù hợp (Improve).

Những phương pháp sau hay áp dụng để bảo vệ hạ tầng ảo hóa và máy chủ ảo: Xác thực và chứng thực: là nhận dạng các dấu hiệu của người dùng thông qua các quyền sử dụng và truy cập hệ thống cũng như dịch vụ. Dữ liệu luôn phải được mã hóa: sử dụng các ứng dụng mã hóa dữ liệu hoặc các thuật toán phù hợp để dữ liệu truyền đi vừa được toàn vẹn vừa an toàn và xác thực, chính xác. Hệ thống tường lửa luôn phải được hoạt động. Triển khai cập nhật để vá lỗi các dịch vụ hoặc ứng dụng đang chạy.

Thực hiện giám sát hệ thống mạng và hạ tầng ảo hóa: hệ thống bảo vệ an ninh của hệ thống mạng xây dựng xong và đưa vào vận hành, việc cần thiết tiếp theo là phải giảm sát hệ thống hoạt động. Theo dõi qua trình đăng nhập, truy cập từ phía người dùng vào dịch vụ, theo dõi hiệu năng hoạt động của hạ tầng ảo hóa. Phát hiện xâm nhập và kiểm soát các chương trình hay dịch vụ lạ bị kích hoạt.

Thực hiện kiểm tra an ninh hệ thống: qua các chính sách và các phần mềm việc rà soát lại các điểm yếu, các chính sách chưa hợp lý, đồng thời thực hiện các cuộc tấn công thử nghiệm để đưa ra các mức đánh giá hệ thống, qua đó đo lường được sức khỏe của hệ thống mạng, hệ thống ảo hóa và các máy chủ ảo hoạt động.

Thực hiện cải tiến hệ thống khi cần thiết: những dịch vụ, phần mềm hoặc các chính sách chạy trên hạ tầng ảo hóa đã bị lỗi thời, việc đưa ra mức độ cải tiến, nâng cấp luôn là điều quan trọng và then chốt. Nó liên quan tới dữ liệu, kinh phí và nhiều chính sách kèm theo. Qua đó chúng ta phải lập kế hoạch rõ ràng trước lúc triển khai.

1.3.2 Những yêu cầu cơ bản bảo mật máy chủ ảo

Khi xây dựng hạ tầng ảo hóa và máy chủ ảo việc người dùng thường xuyên truy cập các dữ liệu để làm việc cũng có nguy cơ mất an toàn dữ liệu. Chúng ta cần đảm bảo các yêu cầu như sau:

Dữ liệu luôn phải sẵn sàng: hệ thống dữ liệu trên máy chủ ảo hay trên máy chủ thông thường cũng đều phải đảm bảo đáp ứng 24/7.

Dữ liệu luôn phải toàn vẹn: khi truy cập hoặc vận chuyển qua đường truyền thì dữ liệu luôn phải được toàn vẹn, không bị chỉnh sửa hoặc bị thay đổi bất hợp pháp.

Các dịch vụ trên máy chủ ảo luôn luôn phải được mã hóa và kiểm soát.

1.4 Tình hình bảo mật máy chủ ảo trong hệ thống Ảo hóa tại Việt Nam và các vấn đề liên quan đến bảo mật máy chủ ảo trong thực tế

1.4.1 Tình hình bảo mật máy chủ ảo trong hệ thống Ảo hóa tại Việt Nam

Công nghệ ảo hóa ngày càng một phát triển, rất nhiều nền tảng khác nhau được tạo ra, vừa thuận tiện cho các doanh nghiệp nhưng cũng tiềm ẩn rất nhiều độ rủi ro và các mối nguy hại xung quang. Việc triển khai Ảo hóa làm giảm chi phí, tiết kiệm được rất nhiều thành phần khác nhau, tăng chế độ hoạt động 24/7, nên mức độ phổ cập tới các doanh nghiệp cũng sẽ rất rộng rãi. Tuy nhiên sẽ có nhiều hệ thống không có chế độ bảo vệ tường lửa, hoặc các chính sách phân quyền, chính sách cho người dùng trên hạ tầng máy chủ ảo, sẽ là nơi béo bở cho các Hacker tấn công hoặc những người tập làm Hacker cũng có thể dễ giàng khai thác. Thực tế ở Việt Nam số vụ tấn công từ bên ngoài Internet vào doanh nghiệp đang là con số khổng lồ, trong lúc mọi người chủ quan là dùng ảo hóa sẽ bảo mật và không ai khai thác được sẽ là rất nguy hiểm. Xét từ hạ tầng ảo hóa tới các dịch vụ chạy trên máy chủ ảo đều có lỗ hổng bở vậy chúng ta cần phải có giải pháp bảo vệ cho doanh nghiệp nếu không sẽ phải chịu hậu quả vô cùng lớn.

1.4.2 Vấn đề liên quan đến bảo mật máy chủ ảo trong thực tế

Những báo cáo thống kê của hãng Microsoft, Việt Nam là những nước đứng đầu trong 05 nước toàn cầu về nguy cơ nhiễm mã độc. Khu vực Đông Nam Á có 02

nước là Việt Nam và Indonesia. Cả hai nước có tỷ lệ bị nhiễm mã độc rơi vào khoảng 46% ở quý II/2016, cao gấp đôi so với trung bình 21% toàn thế giới.

Tại Việt Nam, Cục An toàn thông tin – Bộ Thông tin & Truyền thông đã ghi nhận trong năm 2018 có 10.220 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam. Trong 6 tháng đầu năm 2019 đã có tổng số 3.159 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam.

Thống kê của Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ TT&TT cũng cho thấy, tính từ đầu năm nay đến hết tháng 5/2020, tổng số cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam dẫn đến số sự cố là 1.495 cuộc, giảm 43,9% so so với cùng kỳ 5 tháng đầu năm 2019.

Thống kê của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) ghi nhận 3 tháng đầu năm nay đã có 1.271 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam.

Các thông tin nói trên là rất nguy hiểm nếu hạ tầng ảo hóa phát triển tăng tốc, nhưng các doanh nghiệp không đưa ra được các phương án bảo vệ và bảo mật từ hạ tầng ảo hóa lên tới máy chủ sẽ gây thiệt hại lớn tới doanh nghiệp. Từ đó chúng ta thấy việc bảo mật cho hệ thống mạng nội bộ, hệ thống mạng ảo hóa, máy chủ ảo và các dịch vụ chạy trên máy chủ ảo, tại Việt Nam và trên thế giới càng rất cấp thiết.

1.5 Kết luận chương 1

Chương 1 của luận văn đã nghiên cứu, khảo sát tổng quan về công nghệ Ảo hóa và các các yêu cầu bảo mật đối với máy chủ ảo chạy trên nền tảng Ảo hóa, cũng như tình hình bảo mật máy chủ ảo trong hệ thống Ảo hóa tại Việt Nam và các vấn đề liên quan đến bảo mật máy chủ ảo trong thực tế.

Chương 2: NGHIÊN CỨU GIẢI PHÁP BẢO MẬT MÁY CHỦ ẢO TRONG HỆ THỐNG ẢO HÓA

Chương 2 của luận văn tập trung nghiên cứu các giải pháp bảo mật đối với máy chủ ảo chạy trên nền tảng Ảo hóa.

2.1 Giải pháp sử dụng công nghệ VLAN để tách các Switch ảo trong hạ tầng Ảo hóa (Hypervisor)

VLAN hay còn gọi là Virtual LAN là viết tắt của Virtual Local Area Network, được hiểu là công nghệ mạng LAN ảo. Cho phép tách Switch vật lý thành nhiều Switch ảo logic, tăng độ bảo mật giữa các phòng ban, chống bão Broadcast cũng như thuận tiện quản lý theo từng vùng.

VLAN thường biết tới khi cấu hình trên các Switch Layer 2 hoặc Swtich Layer 3 vật lý. Không những vậy mà trong công nghệ Ảo hóa cũng hỗ trợ các Switch ảo giống hệt logic như Switch vật lý, cho phép tách VLAN, hỗ trợ công nghệ Trunking rất tốt. Trên nền tảng ảo hóa, hệ thống Switch ảo còn cơ động và thuận tiện quản lý, cấu hình hơn cả ngoài Switch vật lý. Số cổng Switch ảo có thể lên tới trên hàng nghìn cổng ảo. Thuận tiện cho chia VLAN trong nhiều trường hợp phức tạp.

Server vật lý thông thường thì Card mạng khoảng 100Mbps, cũng có loại 1Gbps, nhưng đối vưới môi trường ảo hóa các Card ảo thường là 1Gbps và có thể lên tới 8Gbps khi dùng Etherchannel, đây được xem là tính năng rất tốt khi gộp cổng ảo vừa tiết kiệm Card vật lý vừa tăng khả năng xử lý. Ngoài ra những máy chủ quan trọng về dữ liệu ta có thể căm vào một VLAN trong hạ tầng ảo hóa và trỏ Gateway tới cổng của Firewall để đảm bảo hệ thống được bảo mật và an toàn.

2.1.1 VLAN được chia thành 5 loại

- Data VLAN: là VLAN phổ biến nhất, được dùng cho các kết nối của người dùng.

- Default VLAN: là VLAN mặc định tất cả các Switch đều có và khởi tạo tất cả các cổng của Switch đều nằm trong VLAN này. VLAN mặc định của Switch Cisco là VLAN 1 và chúng ta không thể thay đổi tên hay xóa VLAN này.

- Native VLAN: là VLAN duy nhất trên Switch mà Frame xuất phát từ nó khi đi qua đường truyền chung cho các VLAN (đường Trunk) không phải đóng gói thêm trường VLAN ID. Mặc định Native VLAN trên mỗi Switch cisco là VLAN1.

- VLAN quản lý: là bất cứ VLAN nào mà chúng ta cấu hình địa chỉ IP cho interface VLAN tương ứng. Địa chỉ IP này được sử dụng để telnet tới Switch và điều hành hoạt động của Switch từ xa.

- VLAN voice: là một VLAN có độ ưu tiên cao nhất vì Voice là một VLAN ứng dụng thời gian thực. (mạng nghẽn voice vẫn chạy được).

2.1.2 Từ 5 loại VLAN được chia thành 3 kiểu

- Static VLAN: là VLAN tĩnh phân chia theo cổng. Cắm máy vào cổng nào thì nó sẽ theo VLAN đó.

Dynamic VLAN: quy định theo địa chỉ MAC, trên Switch gán MAC: 111111 là của PC1 thuộc VLAN 10 thì Pc1 có cắm vào bất kì cổng nào trên Switch nó vẫn thuộc VLAN 10. Để gán được MAC vào VLAN thì ta phải có một VMPS Server (VLAN Mangerment Policy Server)

- Voice VLAN: chỉ dành riêng cho dữ liệu Voice.

Qua việc phân tích và tìm hiểu về công nghệ VLAN Học viên thấy rất nhiều ưu điểm nên đã lựa chọn công nghệ này: Đa phần VLAN đã tích hợp trong các thiết bị ngày nay và chỉ cần bật lên cấu hình là chạy. Chế độ bảo mật cho các phòng ban là rất cao, tránh được xung đột luồng đi dữ liệu của các phòng ban.

2.2 Giải pháp sử dụng hệ thống phát hiện và ngăn chặn xâm nhập IDS/IPS để bảo vệ hệ thống máy chủ ảo

Trong hệ thống mạng thường có các hệ thống IDS/IPS đặt trên các Firewall cứng. Một số sử dụng Server vật lý để cài các hệ điều hành tường lửa như Pfsense để bảo vệ hệ thống mạng. Đối với hạ tầng vật lý một Firewall sẽ bảo vệ cả một hệ thống mạng bên trong dẫn tới có thể bị chậm hoặc xử lý cùng lúc nhiều tác vụ. Muốn xử lý nhanh thì phải mua những gói License rất cao cho các Firewall cứng.

Để đảm bảo bảo mật cho hạ tầng ảo hóa cần xây dựng một Frewall bảo vệ ngoài cùng, Máy chủ ảo (VPS) bên trong cũng luôn cần riêng một hệ thống tường

lửa bảo vệ chuyên biệt. Lúc này hệ thống VPS cài đặt Firewall như Pfsense sẽ rất hiệu quả. Vừa giúp phân luồng người dùng vừa tập trung đúng vào mục đích sử dụng, tăng hiệu năng và công suất, đồng thời tạo nhiều lớp bảo vệ cho hệ thống máy chủ hơn.

Lúc này Máy chủ cài đặt firewall hoặc Firewall cứng cần có 2 hoặc 3 Card mạng (thường là 3 trở lên), một Card cắm vào cổng External ra ngoài internet, một cổng cắm vào Internal phía mạng người dùng và một cổng cắm vào DMZ khu vực có máy chủ cần bảo vệ. Trên Firewall lúc này ta sẽ bật tính năng IDS/IPS để bảo vệ hệ thống máy chủ bên trong.

Thông qua việc phân tích về IDS/IPS Học viên đã chọn Snort của Pfsense để ứng dụng vì: Snort được tích hợp trên Pfsense nên miễn phí, cộng đồng nguồn mở liên tục cập nhật các chính sách và cơ chế phát hiện mới nhất, hiệu quả cũng được đánh giá rất cao theo tiêu chuẩn bảo mật.

2.3 Giải pháp xây dựng hệ thống tường lửa mềm Fortinet để bảo vệ các máy chủ ảo

Fortinet là bộ tường lửa cứng của hãng FortiGate, được tích hợp rất nhiều tính năng cho phép ngăn chặn và phát hiện hoặc lọc các nguy hiểm cho mạng của công ty rất hiệu quả.

2.3.1 Các chức năng chính của tường lửa Fortinet bao gồm

- Bảo mật kết nối:

+ Chống lại các cuộc truy cập trái phép và phân luồng truy cập.

+ Tạo ra những đường riêng ảo cho phép truy cập bảo mật tơi tài nguyên quan trọng trong công ty.

- Tích hợp bảo mật cho ứng dụng:

+ Kiểm soát các dịch vụ và ứng dụng quan trọng, quét lỗ hổng và đưa ra phương án vã lỗi.

+ Tách và ngăn rất tốt các mã độc lây lan trong mạng.

- Bảo mật ứng dụng:

+ Web Filtering: Ngăn cấm truy xuất đến những địa chỉ đáng ngờ, lừa đảo, spam hoặc chứa nội dung độc hại hoặc chứa các nội dung vi phạm chính sách bảo mật của tổ chức.

+ Antispam: lọc và loại bỏ các thư rác.

+ Kiểm soát ứng dụng: ngăn hoặc giới hạn truyền thông của một số ứng dụng phổ biến (IM, P2P…), có khả năng nhận diện 1800 ứng dụng; kiểm soát lưu lượng ứng dụng.

Đặc điểm nổi bật của Firewall cứng Fortinet vượt lên trên các Firewall mềm (các firewall cài đặt theo dạng ứng dụng trên server) là tính ổn định, khả năng xử lý cao, được chuyên biệt hóa, không giới hạn số lượng người dùng và băng thông lớn. Do đó nó cũng có giá thành khá cao tùy theo cấu hình.

2.3.2 Phân luồng các khu vực

Tuy nhiên, để có thể nâng cao khả năng của firewall, ở các doanh nghiệp hay trường học, nên phân hệ thống mạng ra thành 3 khu vực, gồm:

- Internal: Gồm các máy client bên trong nội bộ
- Perimeter: Gồm các máy chủ của nội bộ như máy chủ web, mail, database,..
- External: Mạng bên ngoài nội bộ

Tại sao lại phải phân ra thành 3 khu vực này. Đó là bởi vì nếu xếp chung các máy chủ và client cùng một khu vực, khi xảy ra sự cố tấn công từ bên ngoài hay phát tán virus từ bên trong, sự cố sẽ lây sang các máy chủ và làm hỏng cả hệ thống mạng.

Firewall Fortinet sẽ đặt nó ở trung tâm, như một cầu nối điều khiển các luồng thông tin cho phép truy cập hay không truy cập.

- Ở Internal, ta sẽ mở firewall cho phép máy bên trong truy cập ra bên ngoài External và Perimeter để lấy thông tin.
- Ở Perimeter, ta sẽ mở cho phép truy cập ra bên ngoài External.

Sau khi cấu hình như trên, có thể giúp hệ thống tránh việc bị tấn công vào server, hay tránh lây nhiễm virus từ các máy client sang server.

Giả dụ, khi trong client gửi một gói tin ra bên ngoài mạng, Firewall Fortinet sẽ mở cổng cho gói tin đó ra ngoài. Sau khi đến server bên ngoài và họ gửi lại một gói tin, firewall sẽ mở cổng để cho gói tin đó đến được máy client vừa mới gửi ra ngoài. Đó là để cho bên trong kết nối ra ngoài mạng bình thường. Nhưng khi xảy ra tấn công, họ sẽ chỉ có thể tấn công vào trong client, nhưng không thể tấn công vào server do ta không có kết nối nào cho phép các gói tin bên ngoài External được truy cập vào trong Perimeter. Việc lây lan virus thông qua các gói tin bên trong mạng nội bộ cũng vậy, do ở khu vực riêng biệt nên sự lây lan sẽ bị giảm thiểu hoặc có thể tránh được nếu phát hiện và xử lý đúng phương pháp.

Sau khi phân tich về tưởng lửa Fortinet, Học viên quyết định lựa chọn vì ch phí đầu tư, xây dựng tường lửa Fortinet là rất phù hợp. Ngoài ra tường lửa Fortinet rất mạnh trong việc lọc và diệt Virus đi qua.

2.4 Giải pháp phân quyền dữ liệu, mở cổng tường lửa cho phép người dùng truy cập thành công từ mạng nội bộ của doanh nghiệp vào hệ thống dữ liệu trên máy chủ ảo

Việc xây dựng tài khoản người dùng của mỗi công ty, doanh nghiệp cho phép quản lý việc truy cập và phân phối các dữ liệu tùy vào từng mục đích cá nhân của những người sử dụng, tránh trường hợp rò rỉ các thông tin quan trọng hay các hoạt động phá hoại dữ liệu khác.

Để vào được hệ thống thì phải đăng nhập bằng tài khoản đăng và mật khẩu. Dựa vào thông tin tài khoản mà hệ quản trị cơ sở dữ liệu sẽ xác minh để cho phép hay từ chối quyền được truy cập vào cơ sở dữ liệu.

Sau khi xây dựng danh sách tài khoản người dùng, chúng ta cần phân tài khoản ra các phòng ban khác nhau tùy vào từng phòng ban một. Việc phân chia vào các phòng ban giúp quản lý các thông tin mà từng nhân viên trong phòng ban đó được phép truy cập hay không. Chẳng hạn ta phân ra 2 phòng ban là IT và Sale, sau đó trên máy chủ ta tạo 2 thư mục cũng là IT và Sale, rồi ta phân quyền cho phép các tài khoản ở 2 phòng ban này truy cập vào thư mục của phòng ban đó nhưng không được truy cập vào phòng ban còn lại. Đó là cách hiệu quả để quản lý dữ liệu, tránh việc thất thoát và các trường hợp không mong muốn.

Do phân theo phòng ban nên các thư mục chứa dữ liệu cũng cần phải được lọc kĩ nội dung để đưa vào các thư mục thích hợp, có hệ thống nhằm dễ quản lý, kiểm soát các đầu mục thông tin theo từng phòng ban.

Ngoài ra hệ thống cơ sở dữ liệu còn xây dựng thêm bản phân quyền truy cập dữ liệu, tùy vào chức vụ như trưởng phòng, giám đốc, giáo viên,… mà ta cho phép các quyền cơ bản đối với dữ liệu là: Đọc, sửa, xóa, bổ sung hoặc không cho phép truy cập. Chẳng hạn nhân viên chỉ được phép xem, bổ sung dữ liệu, còn trưởng phòng mới có quyền sửa, xóa các dữ liệu đó. Đây hay còn gọi là phân tầng quyền truy cập cơ sở dữ liệu.

2.5 Một số giải pháp mở rộng khác

2.5.1 Giải pháp sử dụng phần mềm chống Virus

Rất nhiều kỹ thuật viên của doanh nghiệp bỏ qua bước này, đặc biệt là cài trên máy chủ và máy chủ ảo. Các máy chủ ảo đã tách biệt với hệ thống mạng nội bộ và đưa vào khu vực DMZ, nhưng việc người dùng truy cập tới thì tỉ lệ lây lan Virus qua các File tài liệu vẫn có thể xảy ra cao. Đặc biệt những Hacker họ chèn các Trojan vào trong File và gửi tới thư mục người dùng rồi lây qua File từ người dùng đẩy lên máy chủ ảo. Qua đó chúng ta vẫn phải cần cài chương trình diệt Virus trên máy chủ ảo để quét và đưa ra cảnh báo sớm nhất. Những phần mềm cho máy chủ phổ biến như: BKAV, AVIRA, Kaspersky….

2.5.2 Lập chính sách an toàn thông tin cho hệ thống

Một chính sách an toàn thông tin cho hệ thống (hay còn gọi là chính sách con người) phải gồm nhiều các chính sách được kết hợp với nhau và được tuân thủ nghiêm ngặt để có thể tạo hiệu quả cao nhất. Các chính sách thường có trong một chính sách an toàn thông tin cho hệ thống là:

Chính sách nhân viên nội bộ

- Đầu tiên phải có chính sách cập nhận, câng cao chuyên môn sử dụng công nghệ thông tin và an toàn khi sử dụng Internet. Phải nắm được phương pháp không để lộ mật khẩu, phương pháp kiểm tra link gán Trojan, và tuyệt đối không đăng

nhập vào những trang web đen, web phản động…. Đồng thời đào tạo nâng cao kỹ năng sử dụng nghiệp vụ máy tính.

- Phân quyền thư mục cho các phòng ban, hướng dẫn và nắm bắt được cách truy cập dữ liệu.

- Đưa ra những chế tài, những quy định bằng văn bản để mọi người tuân thủ và ký vào đó, khi xẩy ra sẽ xét theo từng quyền lợi, nghĩa vụ để nhắc nhở, xử phạt.

Chính sách cho khách hàng

Khi khách hàng đến doanh nghiệp thì hệ thống phải có những tài khoản đăng nhập riêng, phải đưa vào vùng mạng có hệ thống Firewall kiểm soát cao độ, có chế độc lọc, phát hiện Virus, phát hiện xâm nhập để đảm bảo họ không thể vượt qua được những bức tường bảo vệ hệ thống của doanh nghiệp. Có thể tách VLAN để họ dùng riêng, đặc biệt không cấp tài khoản vào thẳng dữ liệu trung tâm của doanh nghiệp.

Chính sách cho các đối tác

Với đối tác có thể phải cần tới thiết lập một kênh truyền riêng hoặc tạo ra các kết nối bằng VPN và có IPSEC. Ngoài ra những thiết bị của đối tác đem tới cũng phải đặt vào vùng riêng như cắm USB vào máy chủ quét Virus trước rồi mới cho phép sao lưu hoặc Copy tài liệu.

Chính sách Quản lý tài sản và thiết bị

Phải có phần mềm giám sát và quản lý tài sản về cả phần cứng lẫn phần mềm, đối với phần cứng thì quy định máy nào dùng chung, máy nào dùng riêng để tách khu vực. Đối với phần mềm thì phải quy định phòng ban và quyền truy cập, hệ thống ghi log ở các khu vực đó.

Các thiết bị được bàn giao phải có ngày giờ, trạng thái, dữ liệu và một số tính năng kèm theo.

Lắp đặt hệ thống Camera bổ sung cho việc giám sát.

Xác định những rủi ro và nguy cơ từ đó đưa ra phương án cụ thể.

2.7 Kết luận chương 2

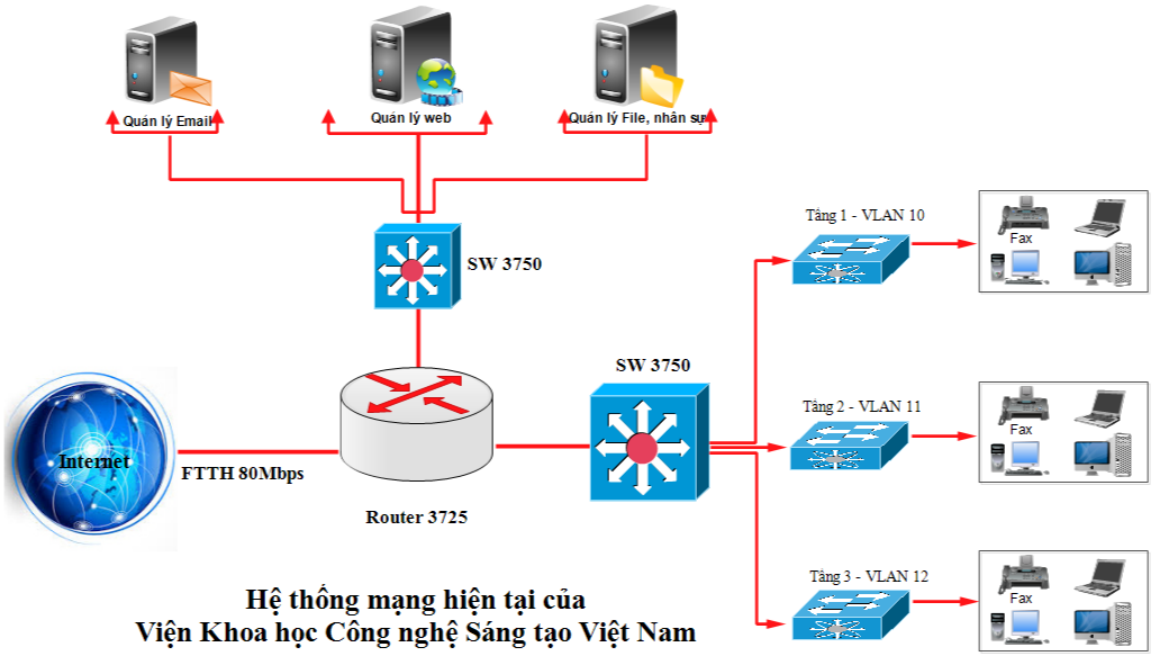
Chương 2 của luận văn đã nghiên cứu các giải pháp bảo mật đối với máy chủ ảo chạy trên nền tảng Ảo hóa và những chính sách hỗ trợ cho người dùng khi truy cập và phải tuân thủ các chính sách an toàn thông tin của công ty. Cần phải phối hợp các chính sách lại tạo chuỗi liên kết thì mới tăng giá trị cao, chông lại mất mát dữ liệu và ảnh hưởng tới hoạt động của doanh nghiệp.

Chương 3: ĐỀ XUẤT GIẢI PHÁP BẢO MẬT MÁY CHỦ ẢO TRONG HỆ THỐNG ẢO HÓA TẠI VIỆN KHOA HỌC CÔNG NGHỆ SÁNG TẠO VIỆT NAM

Chương này sẽ khảo sát về hệ thống Ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam và đề xuất ứng dụng, xây dựng cũng như đưa các giải pháp đã nghiên cứu trong chương 2 cho hệ thống máy chủ ảo tại Viện Khoa học công nghệ sáng tạo Việt Nam.

3.1 Khảo sát thực trạng thực tế về hệ thống Ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam

3.1.1 Chức năng, trang thiết bị và mô hình hiện có của hệ thống mạng Viện Khoa học công nghệ sáng tạo Việt Nam



Hình 3.1: Mô hình mạng hiện tại Viện Khoa học Công nghệ Sáng tạo Việt Nam

Hệ thống mạng hiện tại đang sử dụng kiến trúc mô hình mạng Client - Server nhằm chia sẻ dữ liệu từ các máy chủ tới các máy con. Với kiến trúc mạng hình sao ở các tầng, ta sẽ đạt được tốc độ nhanh nhất có thể, kiểm soát tốt khi xảy ra lỗi cũng như mở rộng tùy ý muốn trong toàn hệ thống.

Hạ tầng mạng được phân cấp: máy tính của các phòng ban sẽ kết nối tới các Switch của các tầng, từ Switch các tầng kết nối tới Switch tổng của tòa nhà. Switch tổng kết nối tới Router 3725 rồi ra ngoài Internet.

Hệ thống máy chủ Web, Mail, File kết nối vào Core Switch. Hệ thống Core Switch kết nối ra Router 3725 để ra ngoài Internet.

- Số lượng phòng ban và các đơn vị trực thuộc sử dụng máy tính là 7.
- Tổng số máy tính cho cán bộ nhân viên là 110.
- Số lượng máy chủ là 08 máy đặt tập trung: 2 máy quản lý File Server, 3 máy chủ chạy Website của Viện (https://www.victs.vn) và các phòng ban, 3 máy chủ chạy dịch vụ: Email, DHCP và DNS.
- Số lượng Switch layer 3 là: 2 Switch 3750
- Số lượng Switch ở các tầng là 6 Access Switch.
- Số lượng tổng đài nội bộ dùng IP là 1
- Số lượng Camera sử dụng 18 chiếc.
- Số lượng đường truyền là 1 ra ngoài Internet: Fpt (FTTH)

3.1.2 Yêu cầu sử dụng

- Hệ thống phải luôn kết nối được Internet.
- Hệ thống Firewall phải bảo vệ hệ thống máy chủ và người dùng 24/7 .
- Các dịch vụ File, Mail, Web luôn phải ổn định để cán bộ nhân viên trong Viện có thể sử dụng. Luôn luôn kiểm soát được số lượng người truy cập dịch vụ.
- Dữ liệu tại các phòng ban phải được tập trung, không phân tán, dễ quản lý, được phân quyền phù hợp với chức trách.
- Khả năng cung ứng cao, đáp ứng được một lượng lớn kết nối vào trong hay ra ngoài mạng mà vẫn giữ được sự ổn định.
- Tiết kiệm điện năng và các chi phí tối ưu nhất cho phòng máy chủ.
- Phải có sao lưu và Backup dữ liệu nhanh chóng.
- Thuận tiện mở rộng hệ thống trong tương lai.

3.1.3 Hiện trạng các vấn đề liên quan trong quá trình vận hành, khai thác mạng máy tính tại Viện Khoa học Công nghệ Sáng tạo Việt Nam

- Hệ thống hiện tại hoạt động rất ổn định và chưa xẩy ra sự cố gì lớn, nhưng hiện tai hệ thống không có Firewall để bảo vệ hệ thống mạng LAN và hệ thống máy chủ. Khi có những Hacker hoặc một số người có ý đồ xấu tấn công thì hệ thống không có phương án hoặc giải pháp phòng chống cũng như đưa ra cơ chế dự phòng.

- Có tới 8 máy chủ chạy các dịch vụ, cũng như các dịch vụ đang chạy là ổn định và rất tốt, nhưng nếu một máy chủ xẩy ra hỏng hóc đột ngột thì dịch vụ đó phải tạm dừng. Ngoài ra khi học viên sử dụng phầm mềm đo lường hiệu năng hoạt động của các máy chủ thì lượng CPU, RAM, Ổ cứng còn trống trên các máy chủ là rất nhiều (chỉ hoạt động tầm 35% công suất so với cấu hình vật lý).

- Ngoài ra hệ thống không có dịch vụ phát hiện tấn công sớm hoặc đưa ra cảnh báo sớm để kỹ thuật viên kịp thời đưa ra những tình huống xử lý làm giảm thiệt hại khi hệ thống bị tấn công.

3.2 Kiến nghị đề xuất các giải pháp bảo mật máy chủ ảo trong hệ thống Ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam

Để đảm bảo bảo mật cho hệ thống và tiết kiệm tài nguyên cũng như nâng cao hiệu quả làm việc của các máy chủ trong hệ thống mạng, tôi xin đề xuất giải pháp như sau:

3.2.1 Giải pháp hạ tầng mạng

Sử dụng Firewall Fortinet 140D thay thế Router 3725, vừa định tuyến vừa bảo mật hệ thống mạng. Trên Fortinet 140D ta tách thành 3 khu vực: mạng LAN, Mạng WAN và DMZ. Khu vực DMZ sẽ xây dựng hạ tầng Ảo hóa rồi tạo ra các máy chủ ảo để cài đặt các dịch vụ.

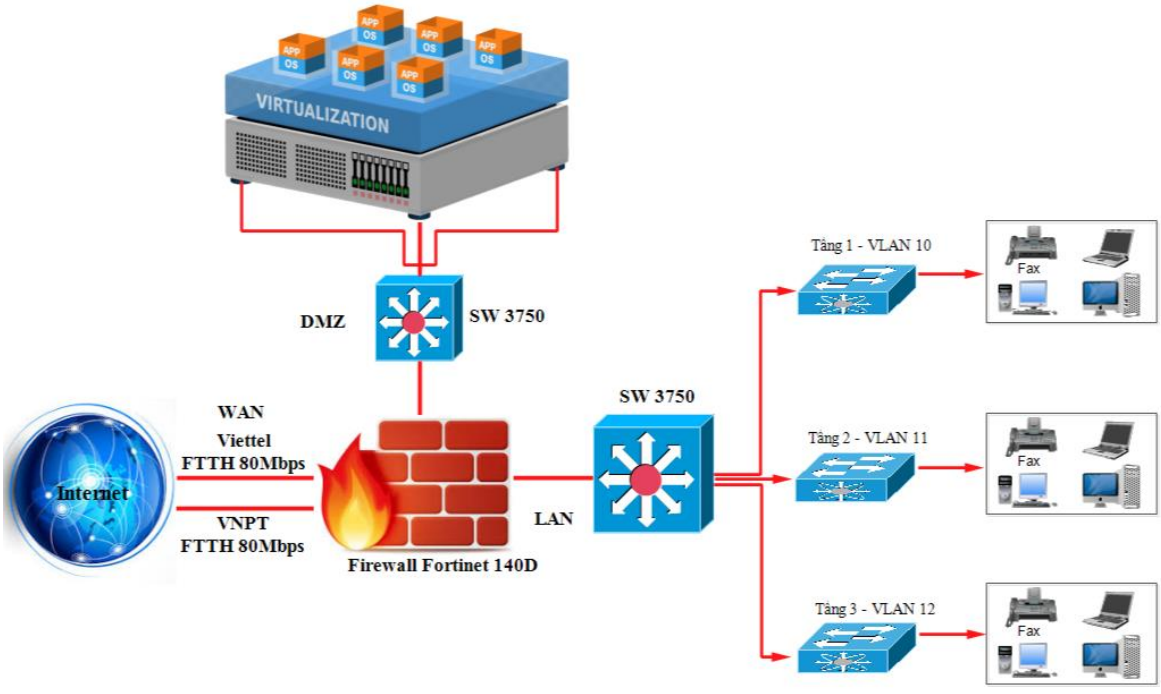
Khu vực mạng LAN đã sử dụng Switch Cisco 3750 có tính năng định tuyến và đã tách VLAN chỉ cần bật tính năng định tuyến đổ về Default Root và trỏ ra cổng kết nối với Fortinet 140D là tín hiệu sẽ truyền về được Firewall.

Khu vực WAN cần bổ sung thêm một đường Internet, một đường bình thường sẽ phục vụ cho mạng LAN đi ra ngoài, và một đường để từ bên ngoài truy cập vào hạ tầng máy chủ ảo, khi một đường xảy ra sự cố thì đường còn lại có thể dự phòng cho nhau tăng tính ổn định.

Đối với khu vực mạng DMZ, trên Switch 3750 ta bật tính năng Default Root và trỏ về cổng kết nối với Fortinet 140D. Đồng thời tách VLAN tương ứng với số VLAN bên trong hạ tầng ảo hóa. Trong hạ tầng ảo hóa ta cũng tách VLAN và bật tính năng Trunking của Switch ảo để đồng bộ với Switch vật lý bên ngoài.

Các máy chủ ảo hóa chỉ cần cắm vào VLAN trong Switch ảo và Port tương ứng là sẽ kết nối được ra ngoài.

Để sớm phát hiện xâm nhập và tấn công (IDS/IPS) vào hạ tầng máy chủ ảo, ta sẽ tạo ra một máy chủ ảo và cài tường lửa mềm Pfsense, sau đó cài đặt Snort trên Pfsense, lắng nghe trên Switch 3750.



Hình 3.2: Hệ thống mạng dự kiến của Viện Khoa học công nghệ Sáng tạo Việt Nam

3.2.2 Giới thiệu một số giải pháp an toàn dữ liệu

Để đảm bảo an toàn dữ liệu em sẽ dùng một số phương án như sau:

- Thực hiện phân quyền truy cập dữ liệu: Đối với các phòng ban ta sẽ phân quyền tùy theo từng yêu cầu của phòng ban đó. Nhưng chỉ nhân viên trong phong ban đó mới xem được dữ liệu của họ, các phòng ban khác không xem được.

- Thực hiện đặt lịch Sao lưu dữ liệu định kỳ và khôi phục dữ liệu khi bị hỏng hoặc xẩy ra sự cố. Tính năng này có sẵn trên Windows Server và hoạt động rất hiệu quả.

- Đối với máy chủ chạy hệ điều hành Linux thì ta có thể dùng Snapshort trên LVM (Logical Volume Manager).

- Ở từng phòng ban chúng ta có thể đặt mật khẩu hoặc mã hóa dũ liệu cho từng phòng ban đó nếu cần thiết.

- Sao lưu dữ liệu lên Cloud của Google hoặc một số dịch vụ Cloud cũng là một giải pháp rất tốt.

- Ngoài ra cần sử dụng bản quyền cho những phần mềm diệt virus trên máy người dùng cũng như trên máy chủ ảo để tránh bị virus gây hại tới dữ liệu.

3.2.3 Giới thiệu giải pháp cho người sử dụng

- Mỗi người dùng cần phải tự bảo vệ mật khẩu, thông tin về tài khoản trên Local hoặc máy cá nhân được tham gia vào Domain.

Người dùng luôn luôn phải tuân thủ chính sách an ninh của hệ thống một cách nghiêm ngặt, đồng thời kết hợp với những chính sách kỉ luật của Viện khi xẩy ra sự cố liên quan tới người dùng.

Thực hiện ngẫu nhiên những phương án cơ bản như dò xóa file, dò các cuộc tấn công bằng tay để tìm ra thủ phạm ngay bên trong hệ thống.

3.3 Thực hiện thử nghiệm và đánh giá một số giải pháp bảo mật hệ thống Ảo hóa

3.3.1 Những nội dung thực hiện thử nghiệm

- Triển khai tường lửa Fortinet và tách 3 khu vực đồng thời cho phép người dùng từ trong LAN truy cập ra Internet và truy cập vào dịch vụ Web trong hệ thống máy chủ ảo, đồng thời Public Web ra ngoài Internet.

- Cài đặt hạ tầng ảo hóa bằng VMWare ESXi, Vcenter bản 5.5

- Cấu hình VLAN trên Switch 3750 khu vực DMZ và đồng bộ với Switch ảo trong hạ tầng ảo hóa của VMWare ESXi và VCenter.

- Tạo máy chủ ảo trên hạ tầng ảo hóa.

- Thực hiện cấu hình dịch vụ Snort trên máy chủ Pfsense.

- Phân quyền truy cập dữ liệu trên máy chủ File Server.

- Sao lưu dữ liệu trên File Server.

(1) Triển khai tường lửa Fortinet và tách 3 khu vực

Trong phần thực hiện cấu hình sẽ chia làm 3 khu vực: phía mạng WAN (2 đường mạng), khu vực mạng LAN và khu vực DMZ, tạo các Rule cần thiết.

Quá trình chia các khu vực giúp dễ quản lý luồng truy cập, đồng thời tránh được lây lan trực tiếp mã độc và chống lại những đợt tấn công từ bên ngoài vào hoặc bên trong tới hệ thống máy chủ.

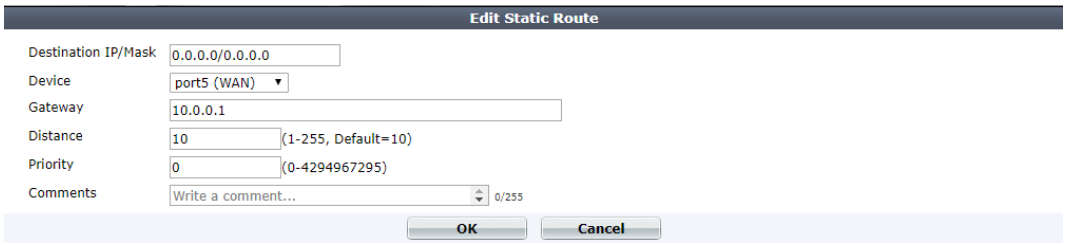
Các bước triển khai:

- Đăng nhập vào Firewall Fortinet sau đó sử dụng câu lệnh "get system interface physical" để xem các thông tin trên Interface. Ngoài ra ta cũng có thể đăng nhập qua giao diện Web để cấu hình. Chúng ta vào phần Interface để cấu hình:

Name		Type	IP/Netmask	Access
port1	(Vlan11)	Physical	11.0.0.1 255.255.255.0	PING, HTTPS, SSH, SNMP, HTTP, TELNET
port2	(Vlan12)	Physical	12.0.0.1 255.255.255.0	PING, HTTPS, SSH, SNMP, HTTP, TELNET
port3	(Vlan13)	Physical	13.0.0.1 255.255.255.0	PING, HTTPS, SSH, SNMP, HTTP, TELNET
port4	(DMZ)	Physical	20.0.0.1 255.255.255.0	
port5	(WAN1)	Physical	10.0.0.20 255.255.255.0	PING, HTTPS, SSH, SNMP, HTTP, TELNET
port6	(WAN2)	Physical	9.0.0.10 255.255.255.0	PING, HTTPS, SSH, SNMP, HTTP, TELNET

Hình 3.3: Cấu hình các Interface

- Trong Static Router, chúng ta thực hiện cấu hình theo các bước sau:



IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	10.0.0.1	port5
0.0.0.0 0.0.0.0	9.0.0.1	port6

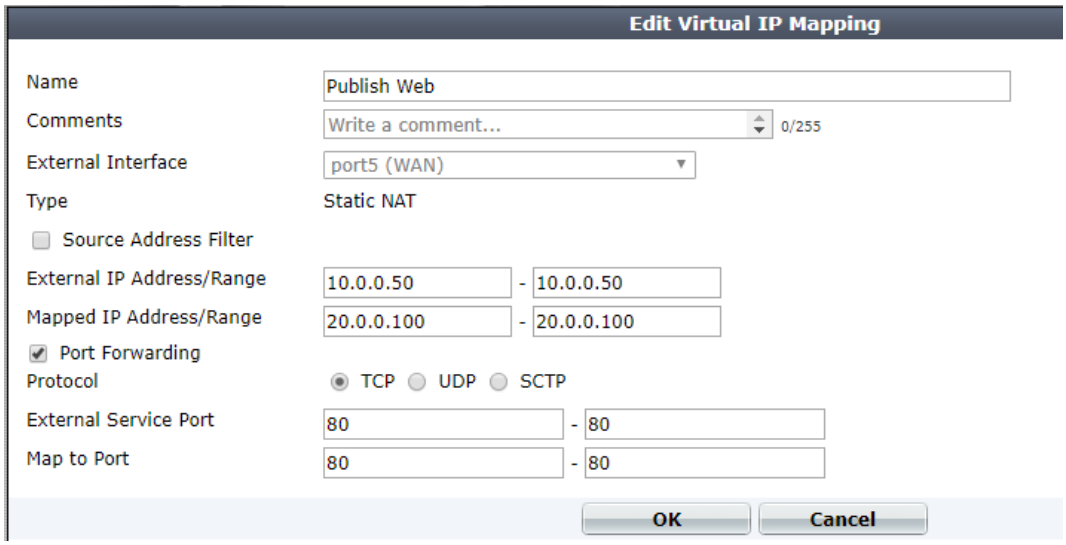
Hình 3.4: Kết quả sau khi chỉnh Static Route

- Trong phần Policy thực hiện thiết lập Rule, mở các kết nối đi từ VLAN sang khu vực DMZ và WAN1, còn từ DMZ ra được 2 WAN (Bật tính năng NAT).

1	port1 port2 port3	port5	all	all	always	ALL		✓ Accept
2	port1 port2 port3	port4	all	all	always	ALL		✓ Accept
3	port4	port5	all	all	always	ALL		✓ Accept
5	port4	port6	all	all	always	ALL		✓ Accept

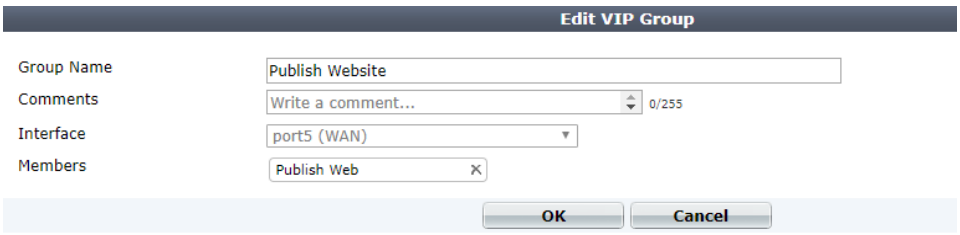
Hình 3.5: Cấu hình các Policy

- Thực hiện Publish Website từ trong DMZ ra ngoài Internet: vào Virtual IPs, thực hiện tạo một Virtual IP Mapping.



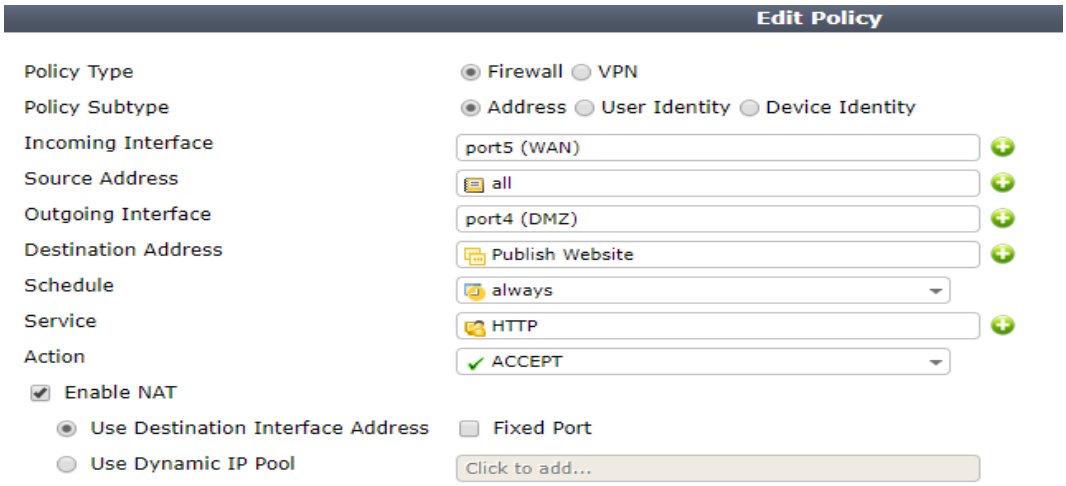
Hình 3.6: Thực hiện Edit Virtual IP Mapping

- Thực hiện Edit VIP Group



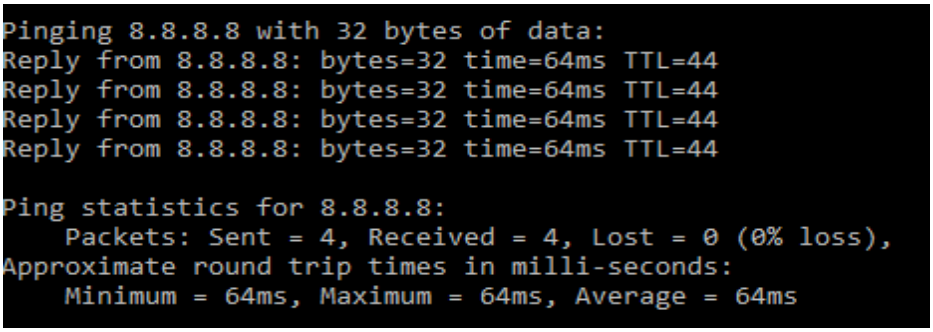
Hình 3.7: đặt tên Publish Website

- Thực hiện thêm Rule mới trong phần Policy để Public Web ra địa chỉ IP bên ngoài.



Hình 3.8: Từ trong DMZ ta thực hiện Publish Web ra ngoài mạng

- Để kiểm tra cấu hình thành công hay chưa chúng ta thực hiện lệnh Ping 8.8.8.8 và sử dụng công cụ Nmap để quét Port đầu ngoài (nếu xanh sẽ là thành công)



Hình 3.9: Sau khi cấu hình Fortinet chúng ta sẽ ping kiểm tra

- Dùng Nmap thực hiện Scan Port ta có kết quả:

Hình 3.10: Test Public Web ở đầu ngoài bằng Nmap.

Khi Public máy chủ ảo cũng thực hiện giống Public Web giúp nhân viên có thể truy cập tới dữ liệu của máy chủ ảo.

Đánh giá giải pháp dựa trên kết quả triển khai:

- Tính chính xác: hệ thống tường lửa của Fortinet đưa ra báo cáo có độ chính xác cao về bảo mật. Giúp phát hiện sớm các cuộc tấn công trực tiếp vào hệ thống.

- Tính hiệu quả: có độ hiệu quả cao, đảm bảo băng thông dữ liệu người dùng ra vào hiệu quả. Khi hệ thống được chia các khu vực giúp dễ quản lý luồng truy cập, đồng thời tránh được lây lan trực tiếp mã độc và chống lại những đợt tấn công từ bên ngoài vào hoặc bên trong tới hệ thống máy chủ.

- Tính bảo mật và an toàn: được đánh giá cao về tính bảo mật, Khi dùng phần mềm Scanport thì các Port đều đóng và đảm bảo yêu cầu.

- Sự hài lòng: giao diện dễ cấu hình và quản trị, tính tương thích cao.

(2) Cài đặt hạ tầng ảo hóa bằng VMWare ESXi, Vcenter

Đầu tiên chúng ta tải file ISO của ESXi 5.5 và File Vcenter 5.5 về, tạo Boot từ CD hoặc USB

Quá trình cài đặt ESXi 5.5

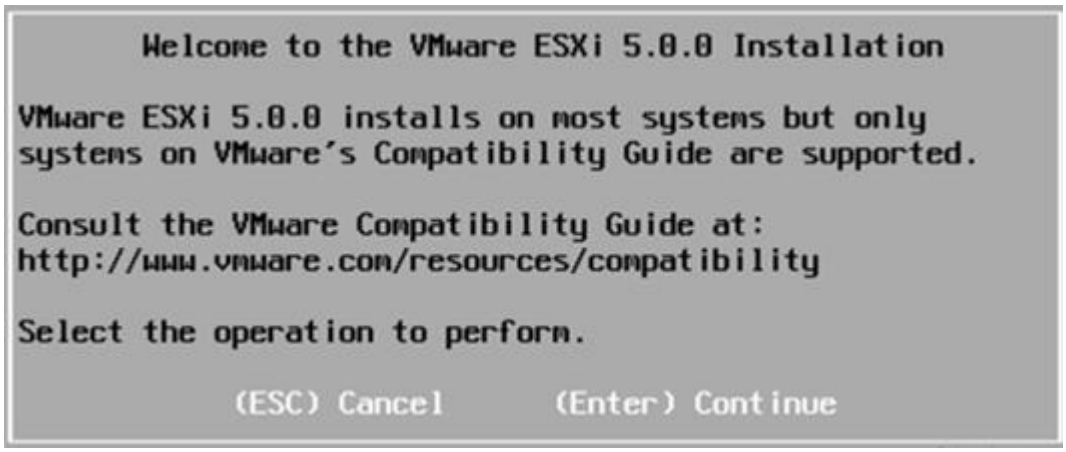
- Load các file cần thiết

Hình 3.11: Load file chính khi cài đặt

- Thông tin phần cứng

Hình 3.12: Thông tin phần cứng được hiển thị

- Nhấn [Enter]

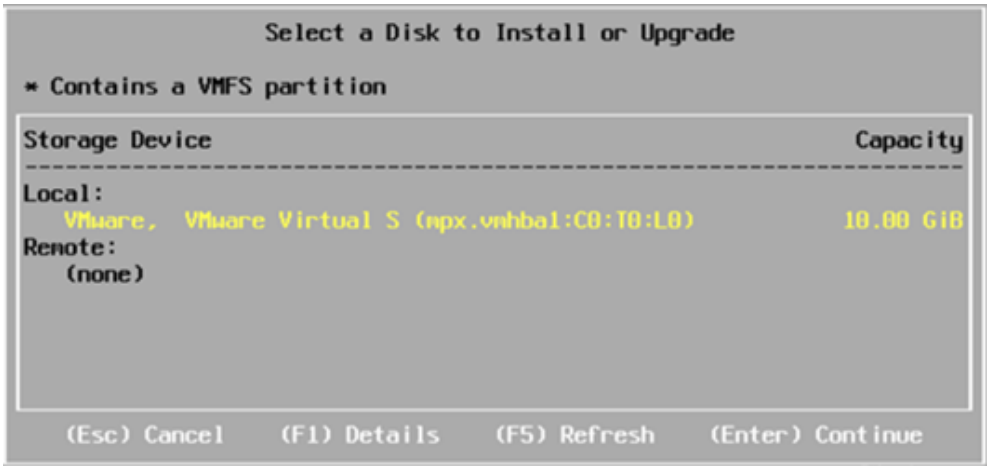


Hình 3.13: Để tiếp tục cài đặt ESXi ta Enter

- Nhấn F11 để đồng ý các điều khoản

Hình 3.14: Chọn F11 để tiếp tục

- Chọn ổ cứng để cài đặt vSphere ESXi 5.0

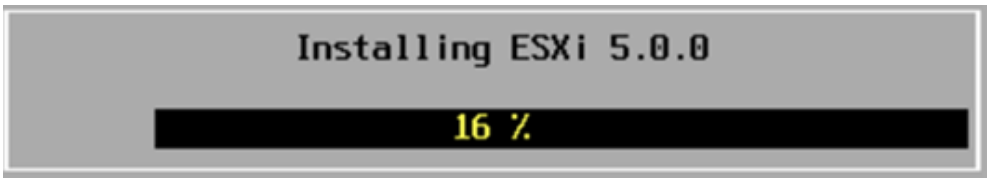


Hình 3.15: chọn ổ cứng để cài đặt

- Sau đó nhập Password cho quyền Root.

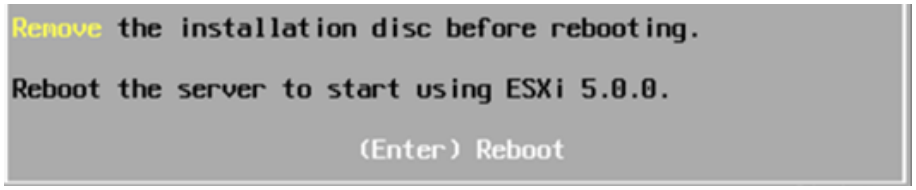
Hình 3.16: nhập mật khẩu cho Root

- Quá trình cài đặt bắt đầu.



Hình 3.17: Quá trình cài đặt được thực hiện

- Sau khi cài đặt xong chọn Enter để khởi động lại



Hình 3.18: Sau khi cài đặt xong tai khởi động lại

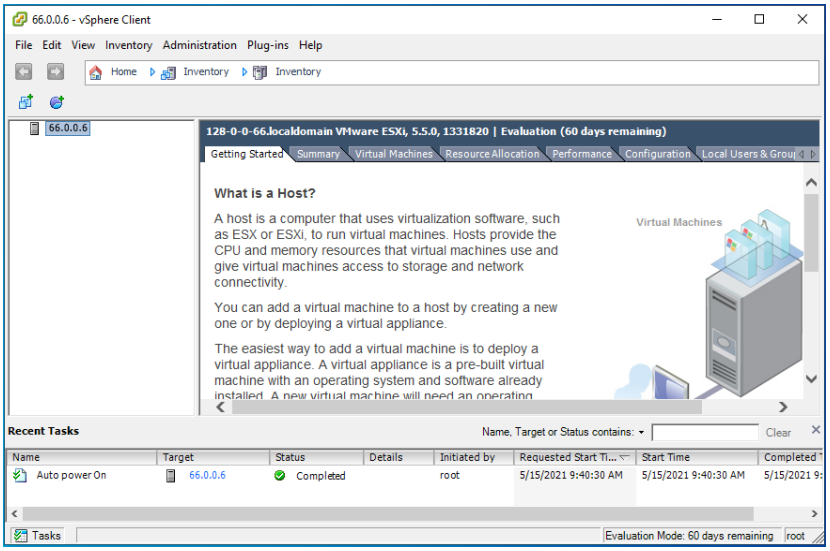
- Sau khi khởi động lại bạn vào cấu hình Card mạng

Hình 3.19: chọn Configure Management Network

- Cấu hình Ipv4 cho ESXi Server: 66.0.0.6/24

- Cấu hình DNS trỏ về 8.8.8.8

- Sau khi cấu hình xong thì khở động lại và dùng vSphere Client kết nối vào hệ thống máy chủ ESXi ta có kết quả:



Hình 3.20: Sau khi cài đặt thành công ESXi và kết nối từ vSphere Client

Quá trình cài đặt Vcenter 5.5

- Cần chuẩn bị một Hệ điều hành Windows Server 2012

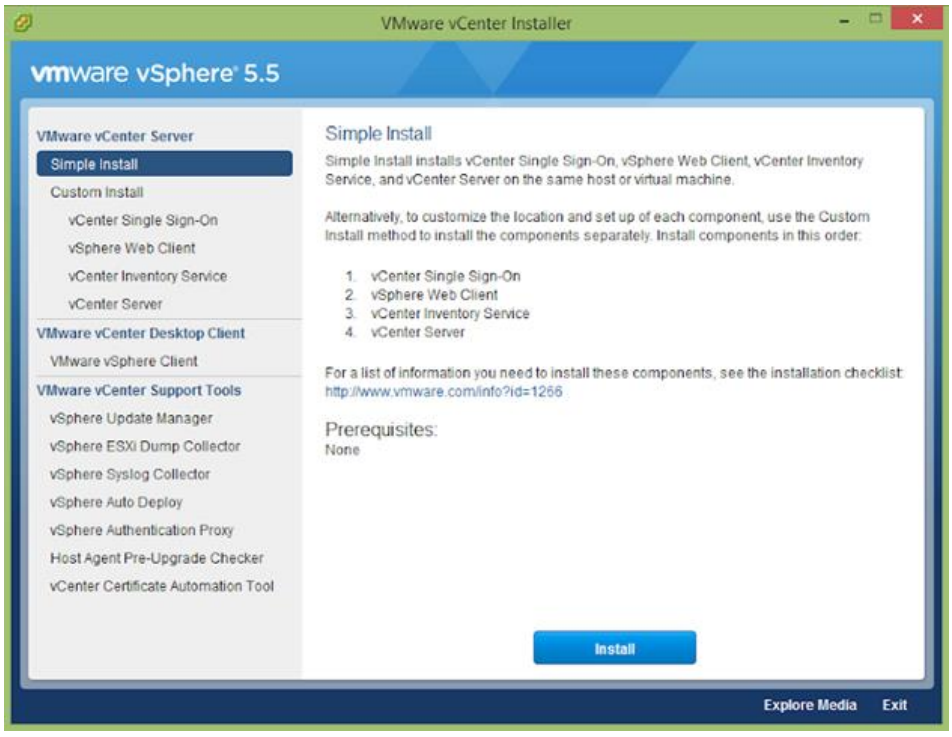
- Yêu cầu phần cứng

Để cài vCenter 5 Chúng ta tạo một máy chủ tối thiểu có: 2 CPU 64-bit hoặc 1 CPU 64-bit core i3 hoặc hoặc cao hơn.

Ngoài ra có thể cài vCenter lên 1 Server vật lý hoặc 1 Server ảo, chúng ta nên có tối thiểu 4Gb RAM nếu chỉ cài vCenter Server,

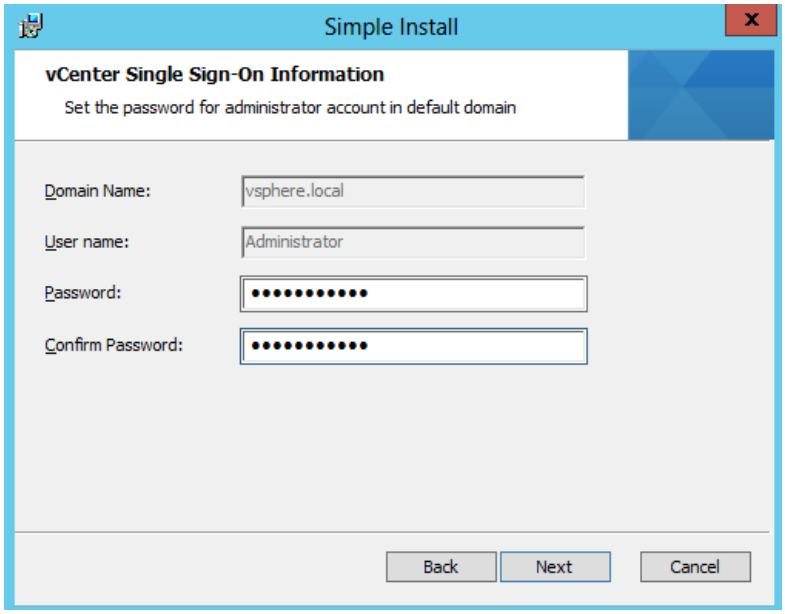
Chúng ta cần 4GB ổ cứng nếu chỉ cài vCenter Server, 60 – 100GB nếu vCenter Server, vCenter Single Sign-On và vCenter Inventory Service cùng cài đặt lên cùng 1 server. yêu cầu đĩa cứng có thể còn cao hơn nữa nếu database của chúng ta cùng trên server này.

- Cho File Boot bằng USB hoặc file ISO vào tiến hành cài đặt



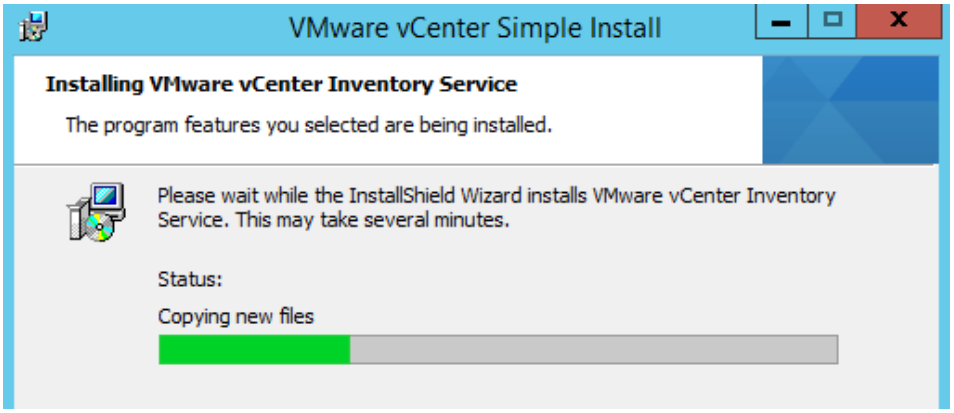
Hình 3.21: Cài đặt Vmware vCenter

- Chúng ta đặt mậu khẩu cho tài khoản Administrator



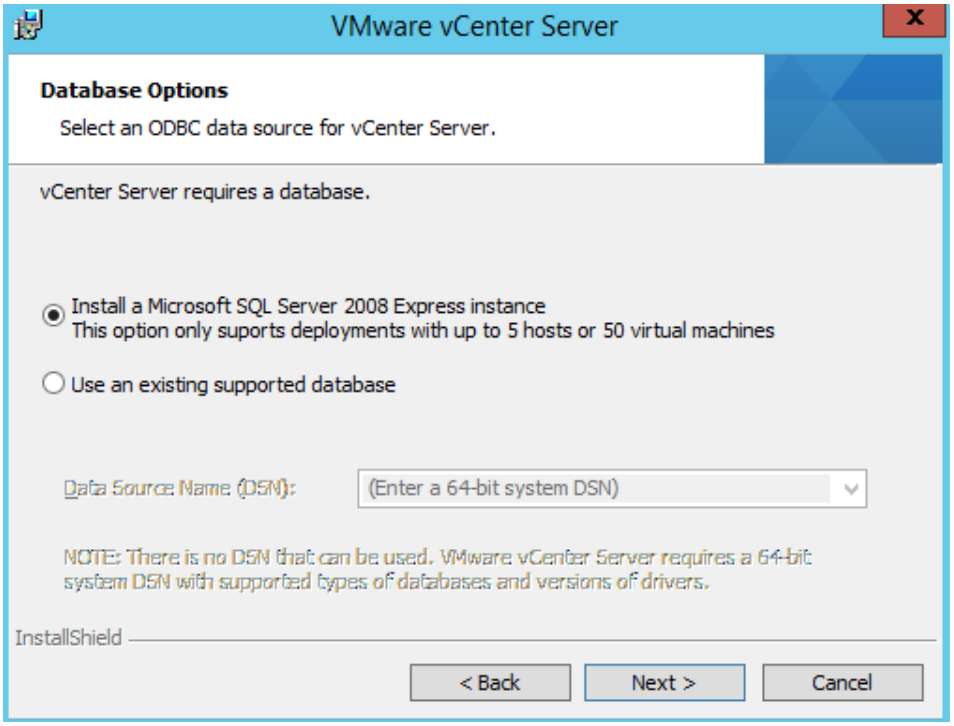
Hình 3.22: Đặt mật khẩu cho tài khoản Administrator

- Để tiếp tục quá trình cài đặt ta chọn Next và quá trình bắt đầu:



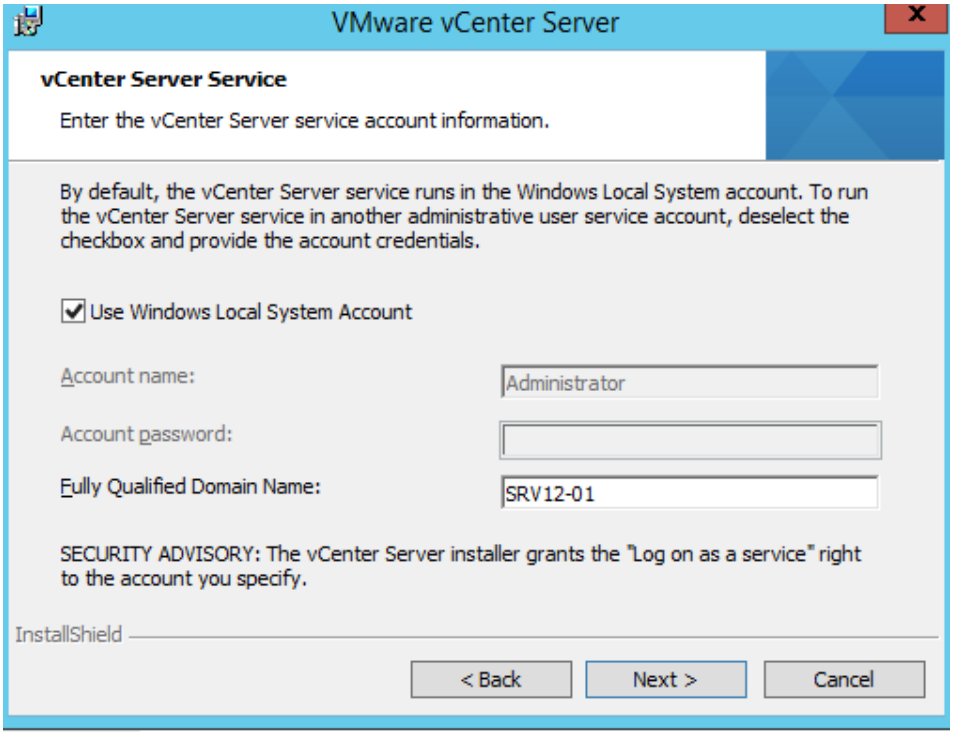
Hình 3.23: Bắt đầu cài đặt

- Tiếp theo chọn Install a Microsoft SQL Server 2008



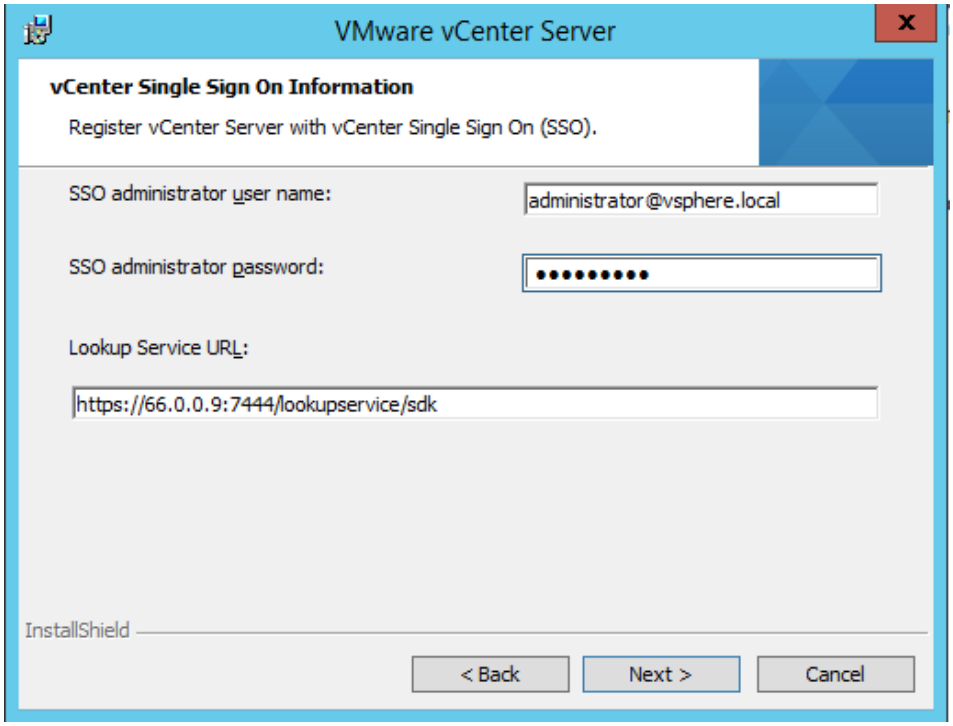
Hình 3.24: chọn vCenDB

- Phần Fully Qualified Domain Name để mặc định và chọn Next



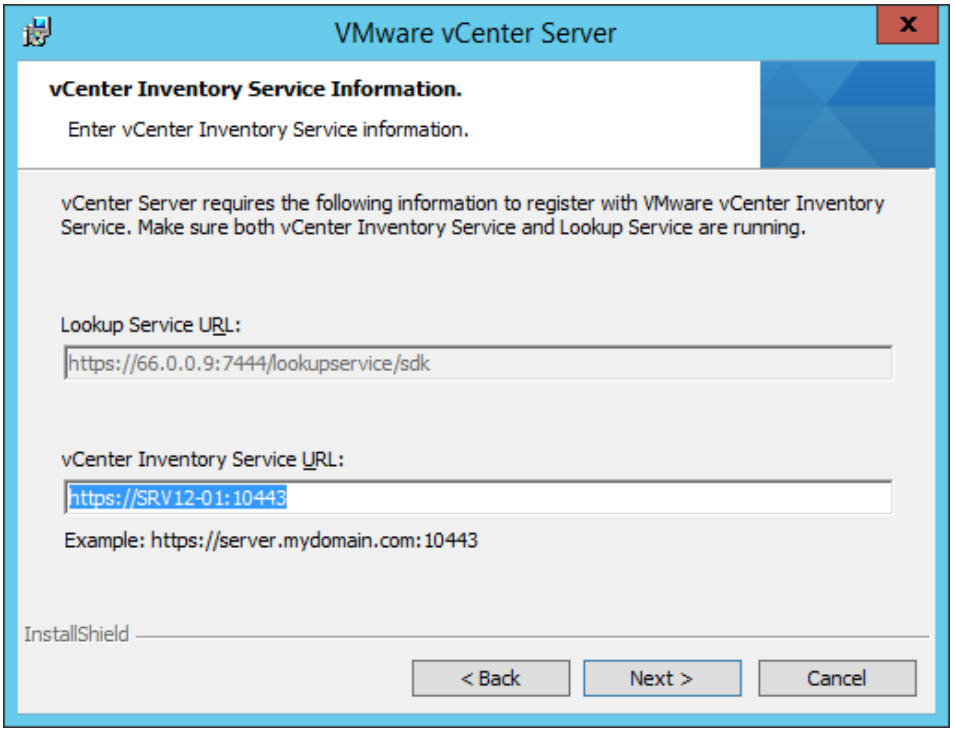
Hình 3.25: Nếu bạn có tên miền đầy đủ thì thực hiện điền tại đây

- Điền mật khẩu Administrator trùng với mật khẩu ban đầu khởi tạo



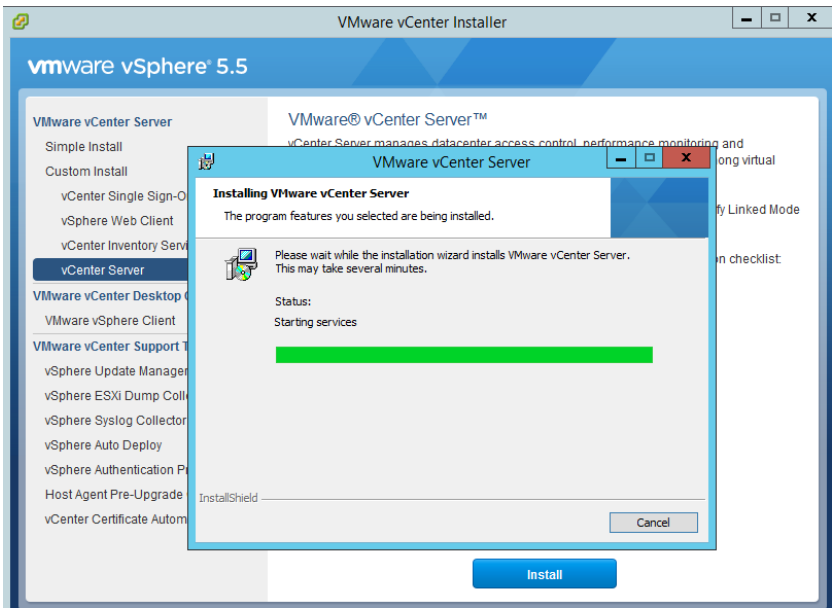
Hình 3.26: Điền mật khẩu Administrator ban đầu khởi tạo

- Trong phần vCenter Inventory Service URL nhớ Port: 10443 chọn Next



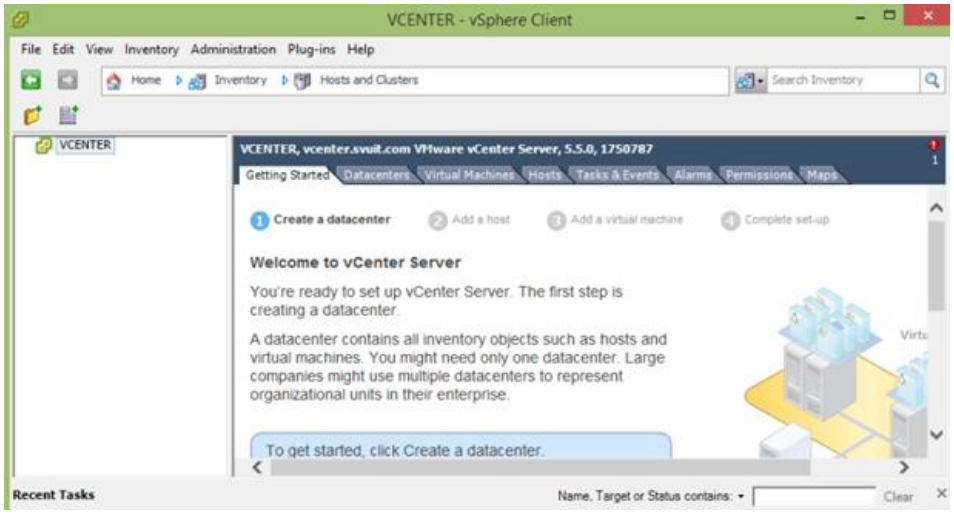
Hình 3.27: Port 10443

- Thực hiện cài đặt vCenter Server



Hình 3.28: thực hiện cài đặt vCenter Server

- Sau khi cài đặt thành công, chúng ta đăng nhập bằn vSphere Client



Hình 3.29: kết quả sau khi cài đặt và đăng nhập thành công

Đánh giá giải pháp dựa trên kết quả triển khai:

- Tính chính xác: khi cài đặt hệ thống rất không xẩy ra lỗi, không phải sửa hoặc bổ sung, tương thích cao với phần cứng.

- Tính hiệu quả: khi tích hợp thành công đem lại hiệu năng hoạt động rất tốt, tạo sự liên kết và dịch chuyển máy chủ trực tiếp mà không bị dừng hoặc treo dịch vụ.

- Tính bảo mật và an toàn: hạ tầng ảo hóa của VMWare được các hãng, các chuyên gia đánh giá là có độ bảo mật cao về cấu trúc hệ thống.

- Sự hài lòng: giao diện đơn giản giúp thuận tiện cài đặt, dễ dùng và quản trị.

(3) Cấu hình VLAN trên Switch 3750 khu vực DMZ và đồng bộ với Switch ảo trong hạ tầng ảo hóa của VMWare ESXi và VCenter

Cấu hình chia VLAN trên Switch 3750

```
SWC(config)#vlan 22
SWC(config-vlan)#name VLAN22
SWC(config-vlan)#vlan 23
SWC(config-vlan)#name VLAN23
SWC(config-vlan)#exit
SWC(config)#
SWC(config)#int range f0/1-5
SWC(config-if-range)#switchport trunk encapsulation dot1q
SWC(config-if-range)#switchport mode trunk
SWC(config-if-range)#exit
SWC(config)#
SWC(config)#int vlan 1
SWC(config-if)#ip add 10.0.0.254 255.255.255.0
SWC(config-if)#ip helper-address 10.0.0.6
SWC(config-if)#no shut
SWC(config-if)#exit
SWC(config)#
SWC(config)#int vlan 22
SWC(config-if)#ip add 22.0.0.254 255.255.255.0
SWC(config-if)#ip helper-address 10.0.0.6
```

SWC(config-if)#no shut

SWC(config-if)#exit

SWC(config)#

SWC(config)#int vlan 23

SWC(config-if)#ip add 23.0.0.254 255.255.255.0

SWC(config-if)#ip helper-address 10.0.0.6

SWC(config-if)#no shut

SWC(config-if)#exit

SWC(config)#

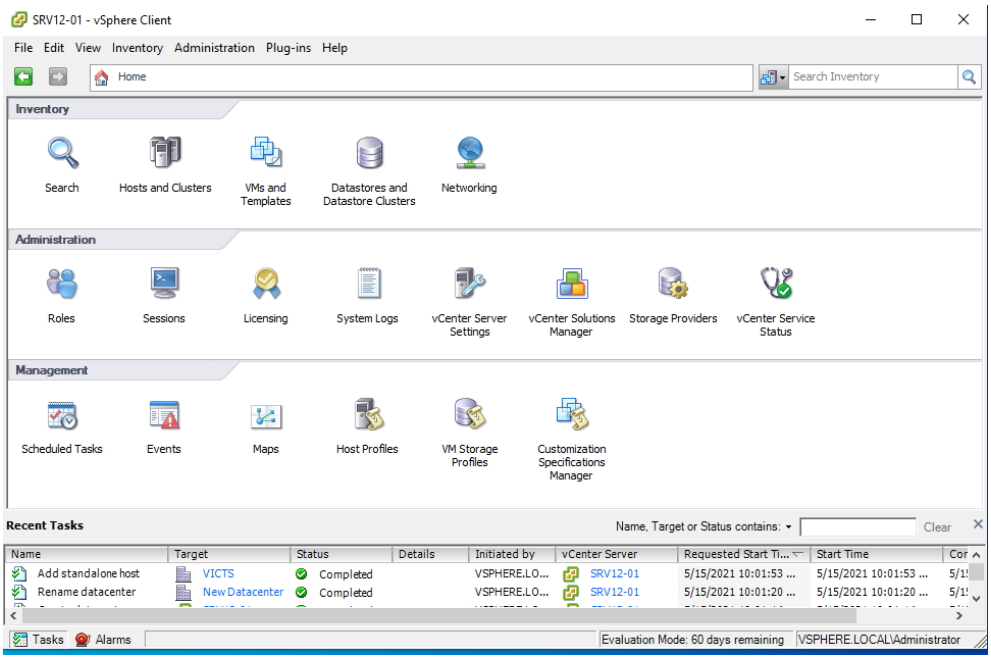
SWC(config)#ip routing (cho phép định tuyến)

SWC(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1 (đường ra Internet VLAN1)

SWC(config)#

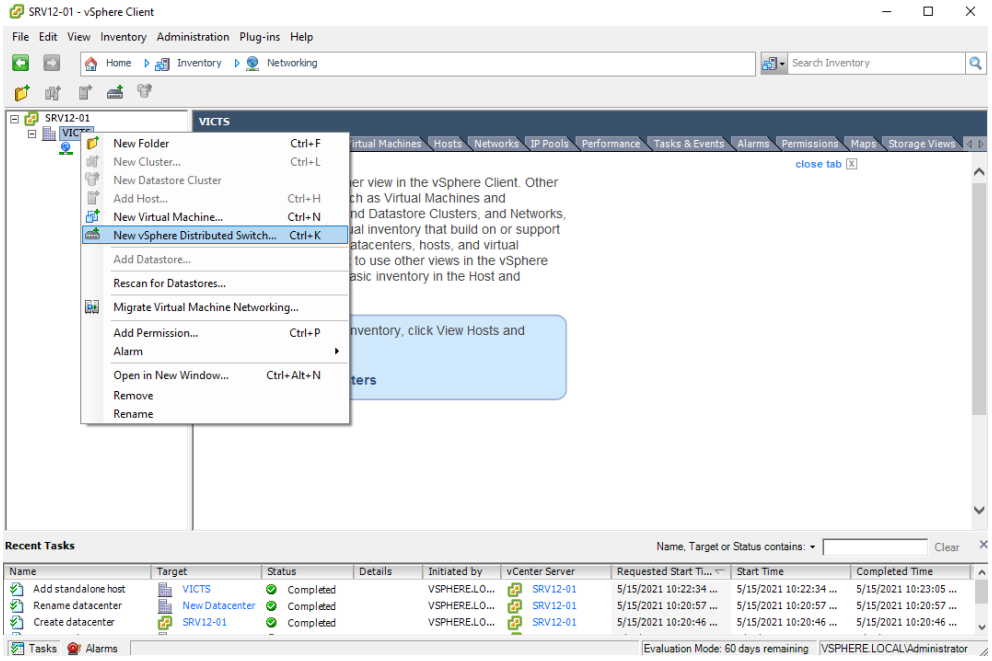
Cấu hình VLAN trên Switch ảo của vCenter

- Trên vSphere Client ta chọn Home rồi chọn Networking



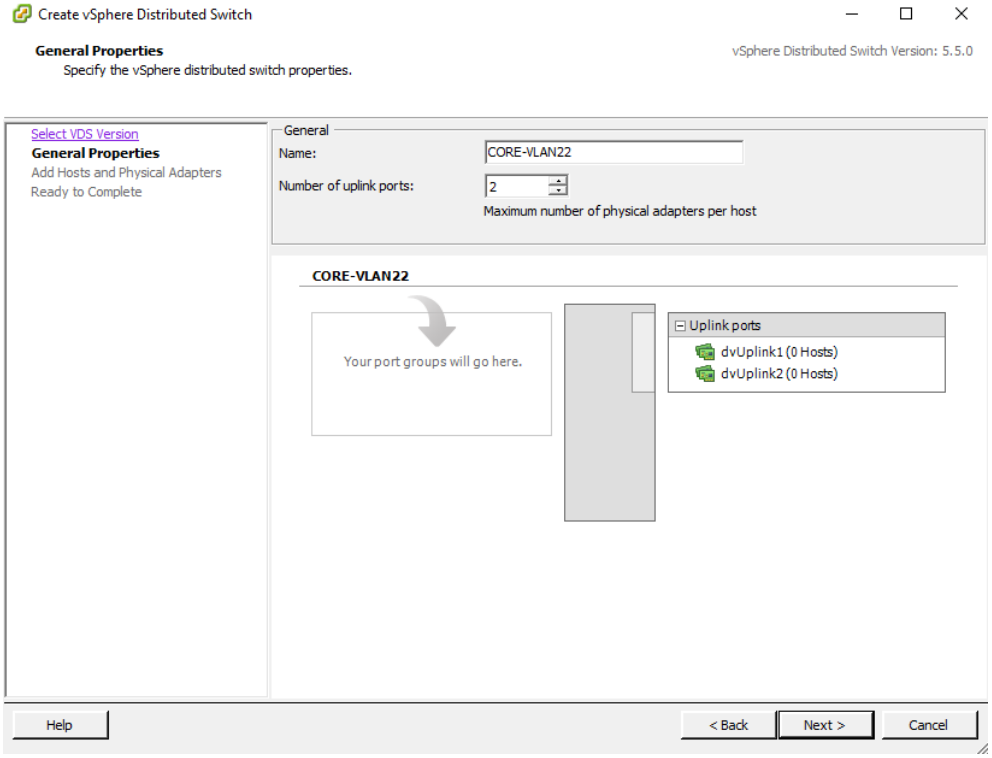
Hình 3.30: chọn Networking

- Tạo Switch ảo đặt tên là VLAN22: Chọn New vSphre Distributed Switch



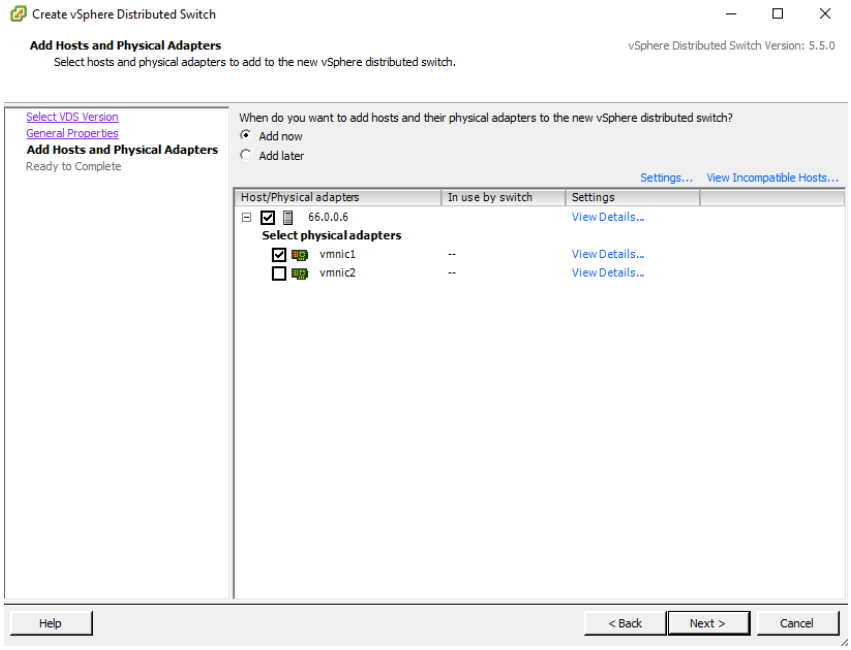
Hình 3.31: Tạo Switch ảo VLAN22

- Đặt tên Switch ảo là VLAN22



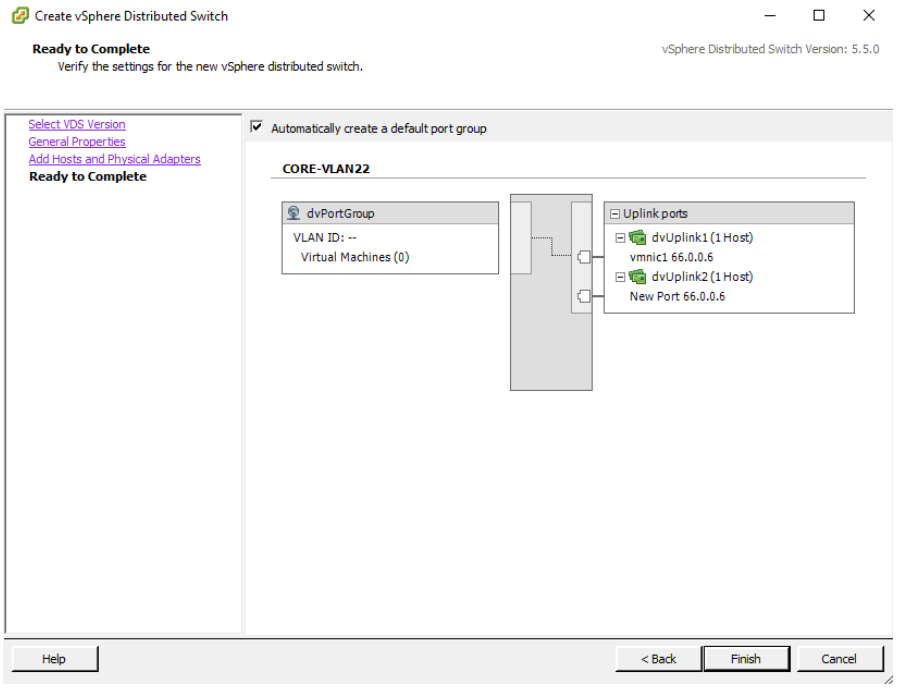
Hình 3.32: Đặt tên cho Core-VLAN22

- Gán Card mạng tương ứng cổng ra Switch vậy lý



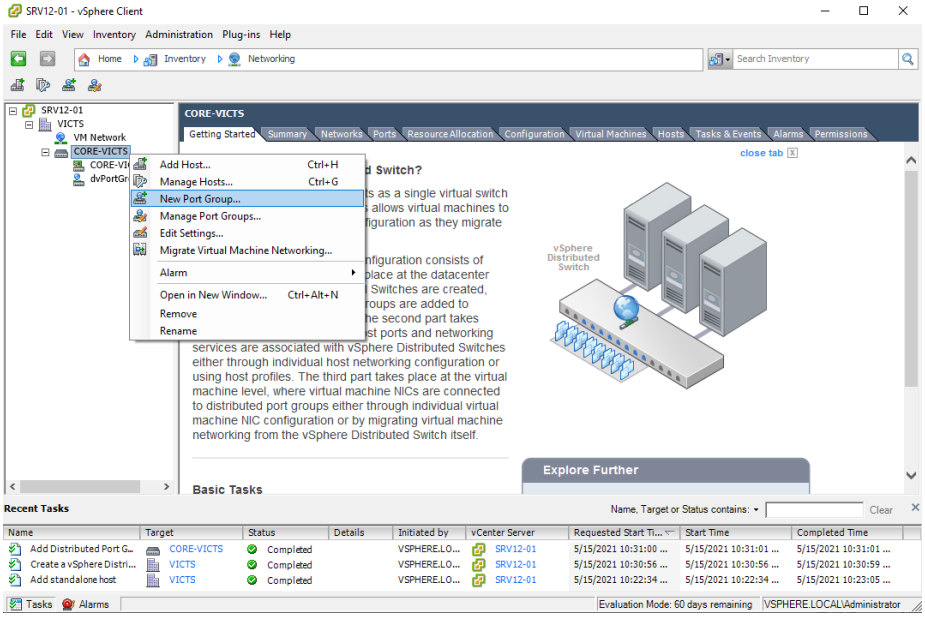
Hình 3.33: gán card mạng vmnic1

- Chọn Finish



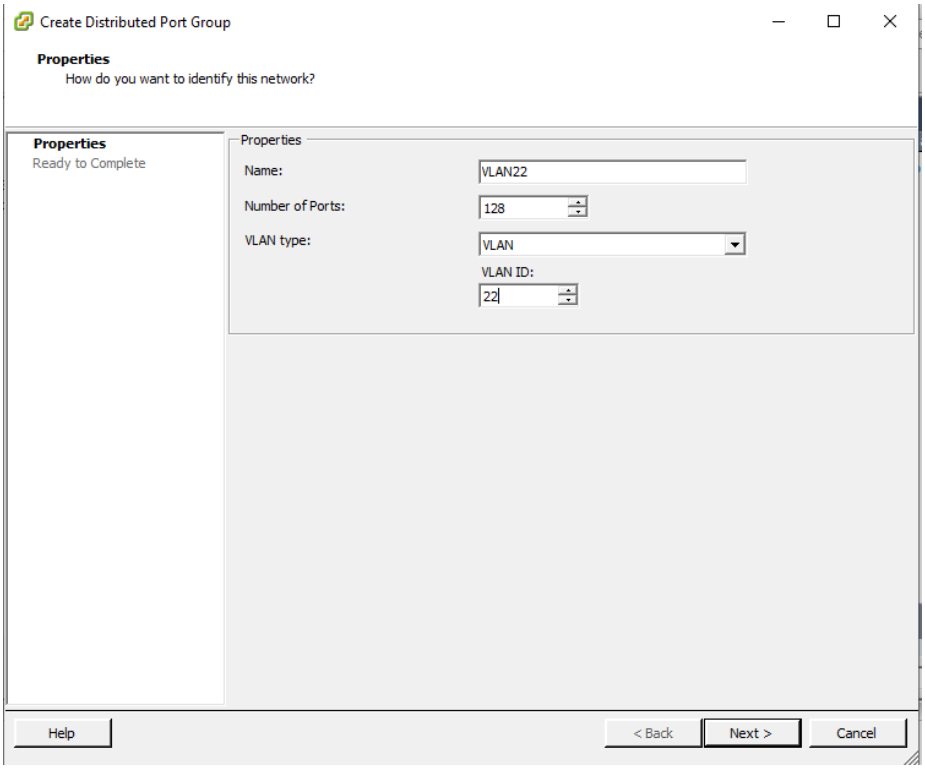
Hình 3.34: Tự động tạo Port mặc định

- Thực hiện tạo Port Group cho VLAN22



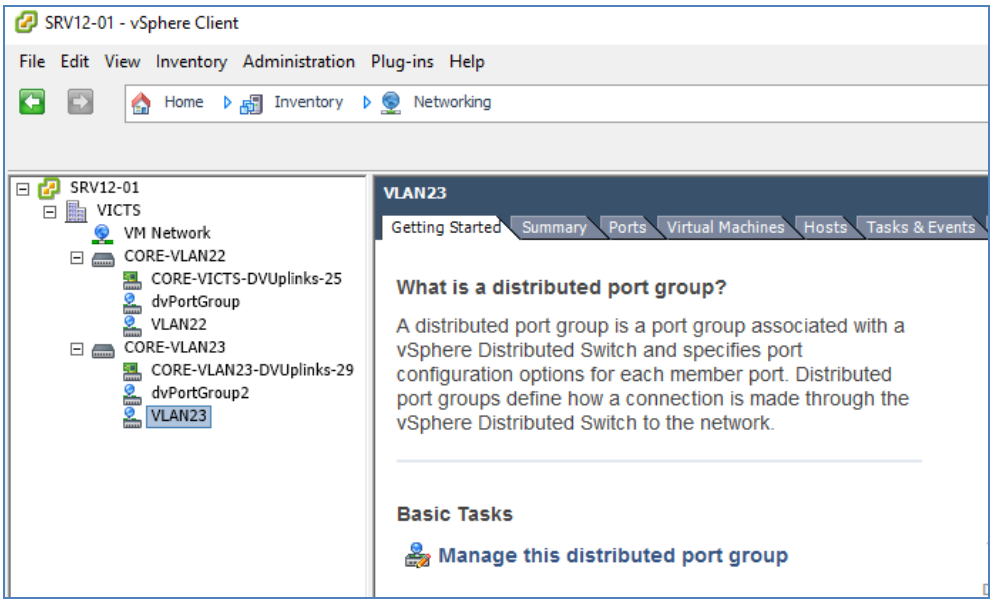
Hình 3.35: Tạo Port Group

- Tạo Port Group cho VLAN22



Hình 3.36: Đặt tên và tạo Port 22

- Tương tự thực hiện tạo VLAN 23



Hình 3.37: Tạo thành công VLAN22 và VLAN23

Đánh giá giải pháp dựa trên kết quả triển khai:

- Tính chính xác: dữ liệu truyền qua kết nối giữa VLAN trên hạ tầng ảo hóa với Switch vật lý ổn định. Sử dụng phần mềm đo lường thấy không bị mất gói tin.

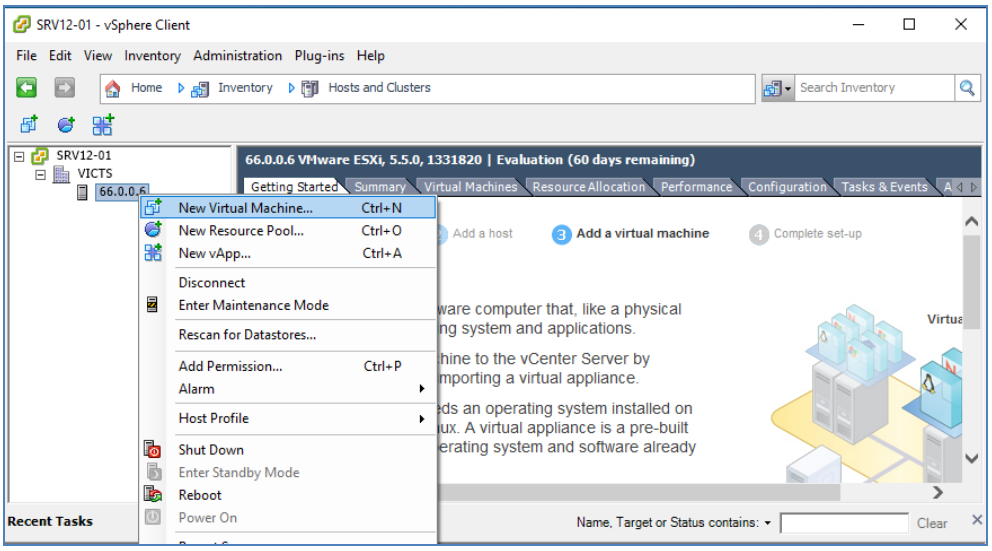
- Tính hiệu quả: Giải pháp này giúp tiết kiệm rất nhiều Switch vật lý. Có thể tăng giảm băng thông lên tới 8Gbps bằng công nghệ etherchannel, cũng như nâng cấp rất thuận tiện.

- Tính bảo mật và an toàn: giữa các vùng khi tách VLAN kết nối theo luồng có độ bảo mật rất cao, người dùng bên VLAN này sẽ không truy cập được sang VLAN khác.

- Sự hài lòng: đồng bộ hạ tâng ảo hóa trên Switch ảo của VMWare và Switch vật lý đem lại giá trị cao và tiết kiệm chi phí cũng như tinh gọn trong hệ thống, thuận tiện trong việc quản trị và điều chỉnh, nhanh chóng khi cần nâng cấp.

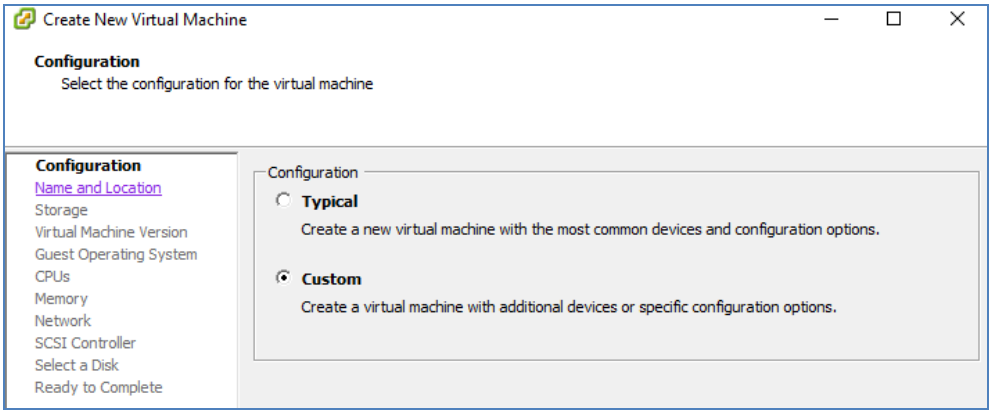
(4) Tạo máy chủ ảo trên hạ tầng ảo hóa bằng vCenter

- Từ Hosts and Clusters chọn Server 66.0.0.6 sau đó phải chuột thực hiện chọn tạo máy ảo mới (New Virtual Machine)



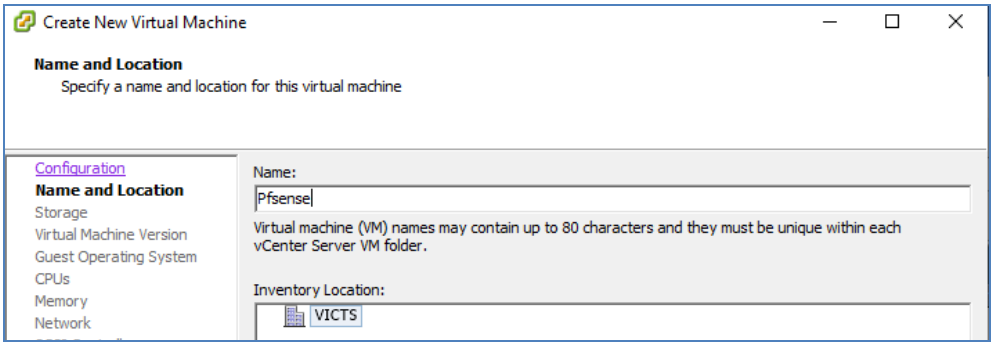
Hình 3.38: Chọn New Virtual Machine

- Chọn trạng thái tùy chỉnh là Custom



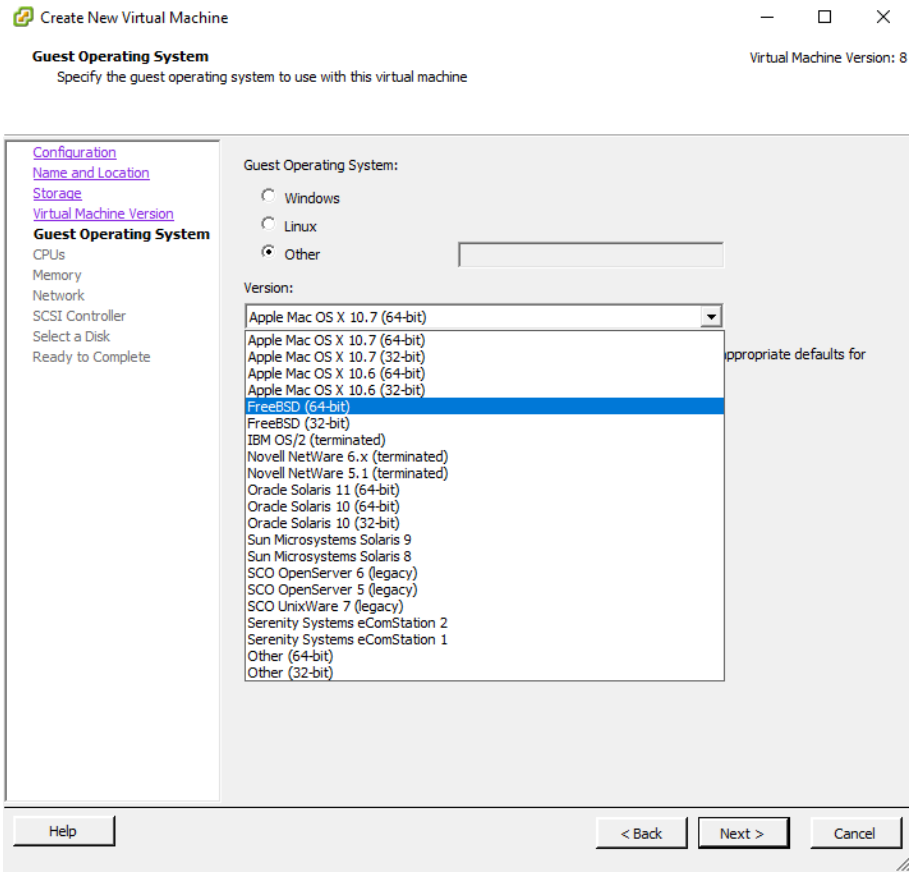
Hình 3.39: Chọn Custom

- Đặt tên cho máy chủ ảo là Pfsense



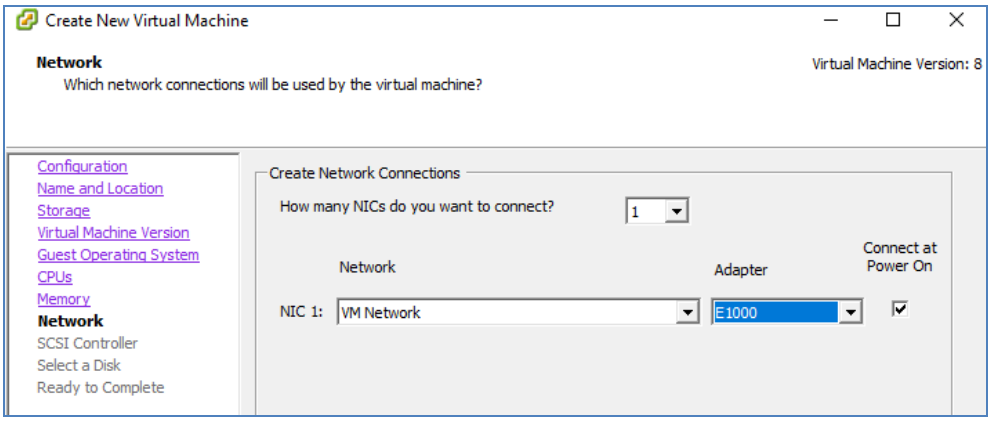
Hình 3.40: Đặt tên cho máy chủ ảo

- Trong Guest Operating System bạn có thể chọn các hệ điều hành Windows, hoặc Linux. Ta cài đặt tường lửa Pfsense sẽ chọn Other và chọn FreeBSD (64-bit).



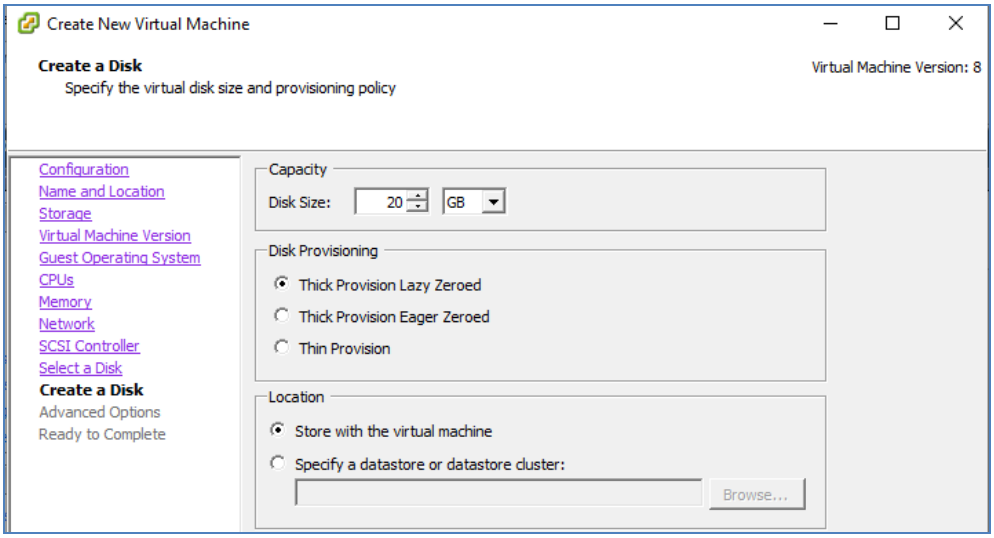
Hình 3.41: chọn FreeBSD 64-bit

Để lắng nghe các cuộc tấn công từ ngoài vào hệ máy chủ ESXi thì chọn VM Network



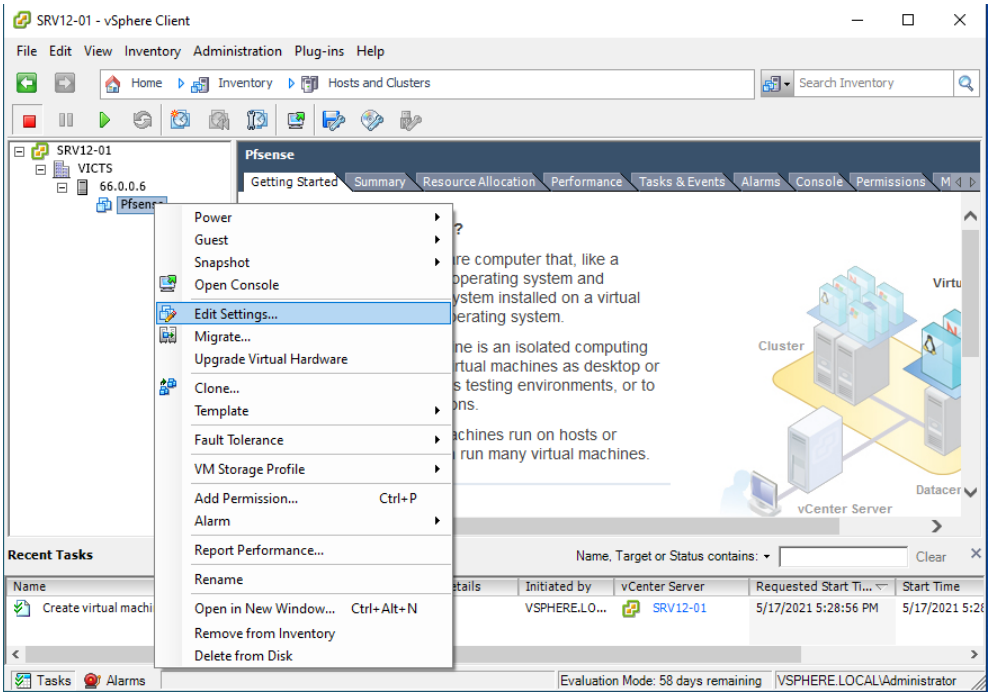
Hình 3.42: lựa chọn cổng lắng nghe

- Chọn ổ cứng là 20G và chọn chế độ gán cứng dung lượng ổ là Thick Provision Lazy Zeroed



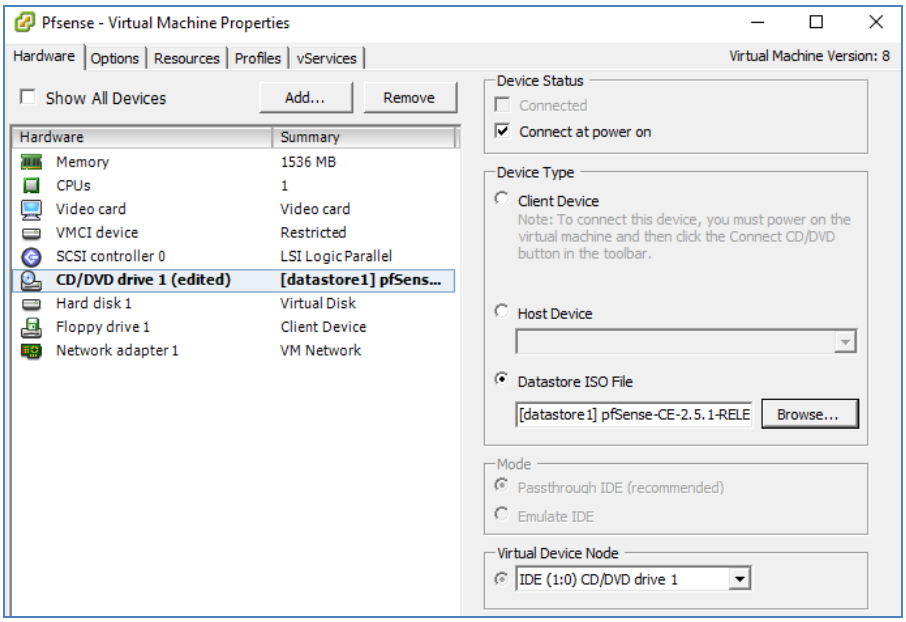
Hình 3.43: chọn chế độ cho ổ cứng ảo

- Sau khi tạo ổ ảo và Finish thì ta vào máy chủ ảo Pfsense chọn chuột phải vào Edit settings



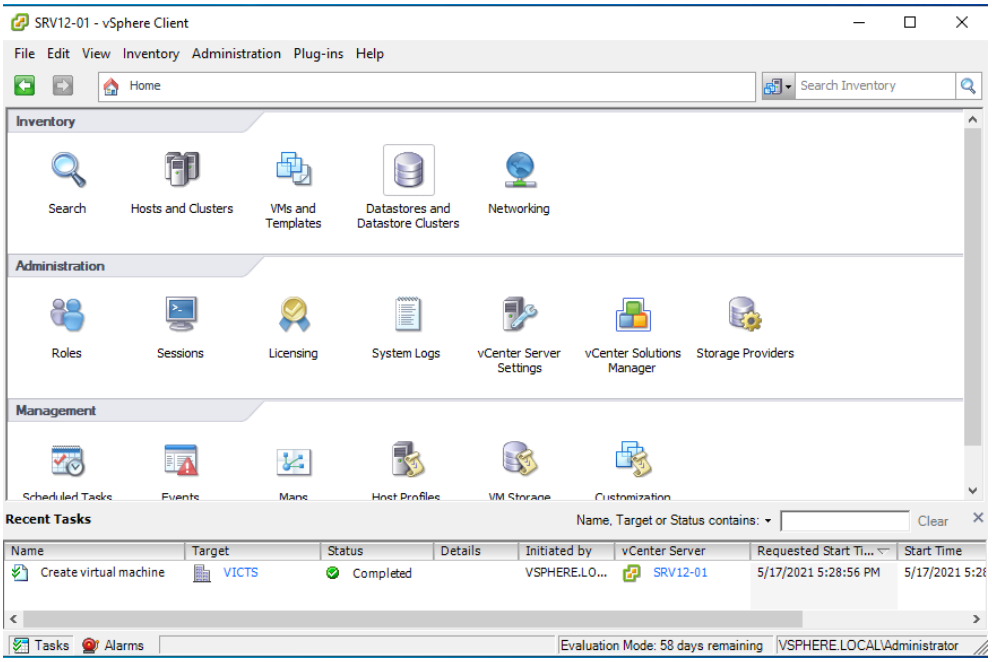
Hình 3.44: chọn Edit settings

- Chọn CD/DVD và tích vào Connect at Power on và tích vào Datastore ISO File và Browse tới File ISO



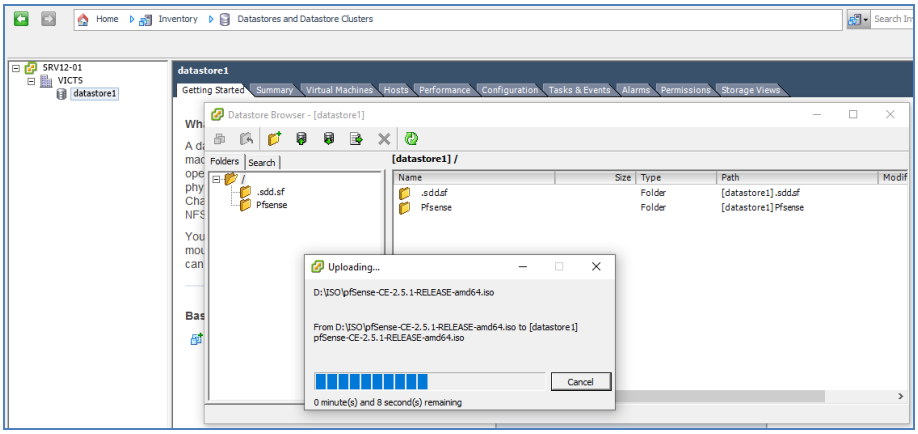
Hình 3.45: chọn Datastore ISO File và Browse tới File ISO

- Để đưa được File ISO vào hệ thống ảo hóa ta chọn Home rồi vào Datastores and Datastore Clusters



Hình 3.46: chọn Datastores and Datastore Clusters

- Chọn Datastore Brower rồi chọn Upload file và đưa file ISO lên

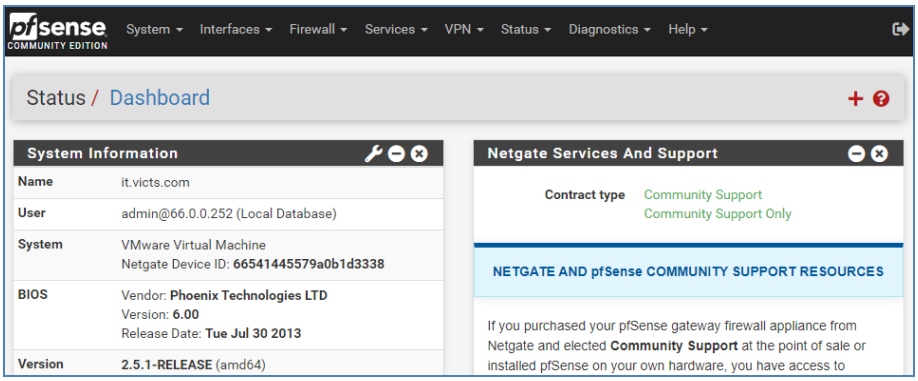


Hình 3.47: Upload File ISO lên hệ thống lưu trữ

- Quá trình cài đặt hệ điều hành Pfsense hoặc Windows Server hoặc Linux từ phần này trở đi đều giống như cái máy chủ bình thường.

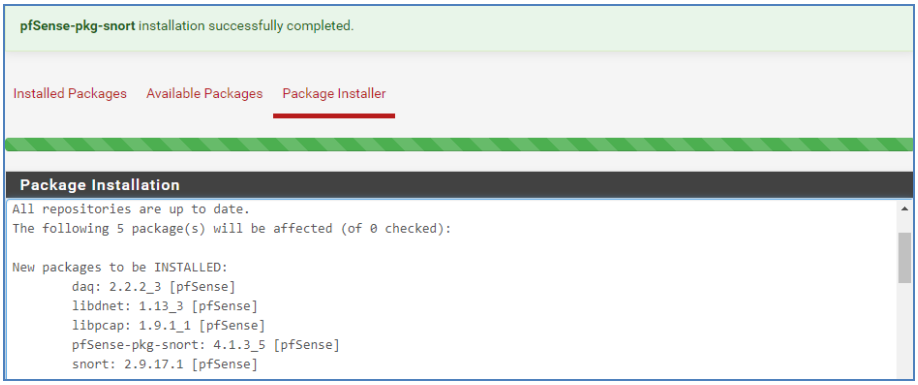
(5) Cấu hình Snort trên Pfsense

- Từ giao diện chính của Pfsense sau khi cài đặt xong ta chọn System và chọn Package Manager rồi chọn Available Packages



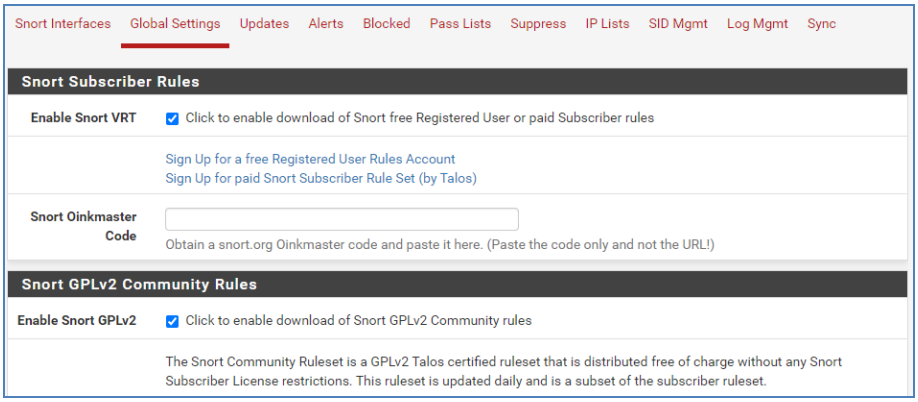
Hình 3.48: Giao diện của Pfsense đăng nhập bằng trình duyệt Web

- Chọn xuống Snort chọn cài đặt.



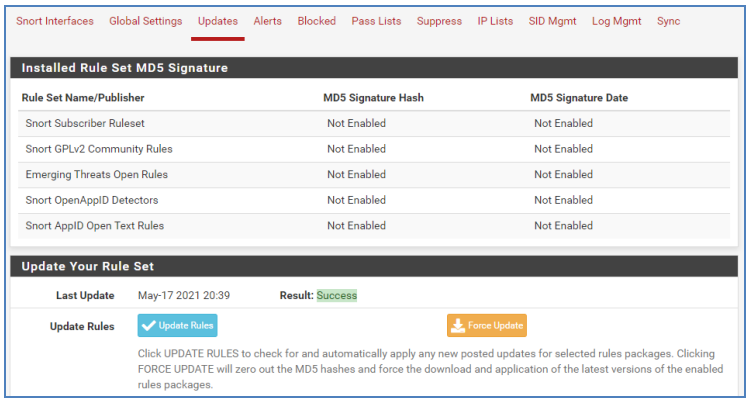
Hình 3.49: Cài đặt gói thành công

- Chọn Global Settings và chọn Rule VRT và GPLv2



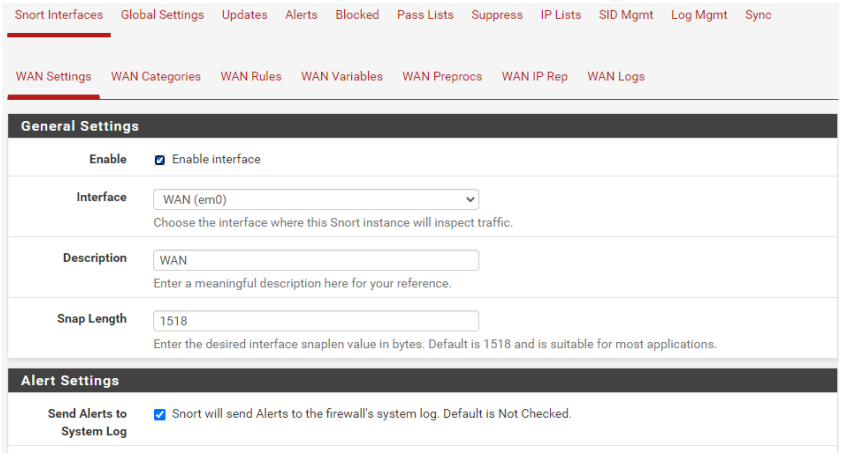
Hình 3.50: Chọn Rule Snort VRT, GPLv2

- Chuyển sang cài đặt và Update Rule



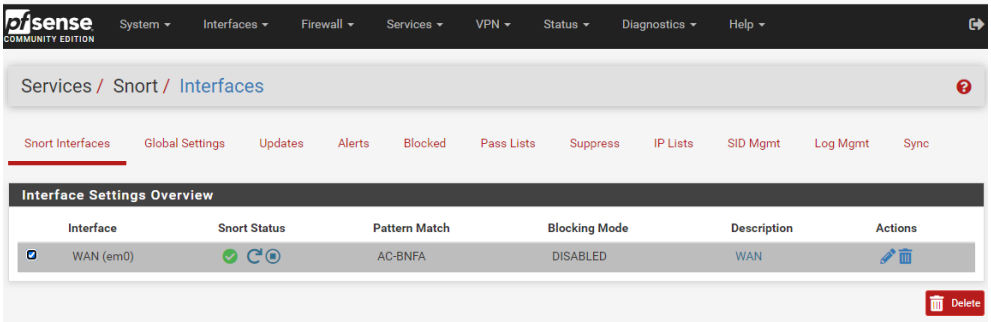
Hình 3.51: Update Rule

- Chọn Snort Interface vào WAN Settings tích vào Send Alerts System Log



Hình 3.52: Bật tính năng gửi cảnh báo

- Sau khi cấu hình xong chúng ta bật trạng thái Snort trên Interface



Hình 3.53: Snort trên Interface WAN đã được bật

Đánh giá giải pháp dựa trên kết quả triển khai:

- Tính chính xác của phần mềm: dựa trên các thông tin từ diễn đàn trang bảo mật và so sánh với hệ thống Fortinet thì độ chính xác của Snort được đánh giá cao.

Snort phát hiện, đưa ra cảnh báo nhanh chóng và ghi lại log. Người dùng truy cập vào dịch vụ bên trong máy chủ đã bắt và ghi được một số địa chỉ IP. Khi đo trên thực tế thì chưa bị nhỡ phiên trong khi truy đo lường.

- Tính hiệu quả: hiệu suất của Snort trên Pfsense tốt, chịu tải được nhiều truy cập trực tiếp đi qua (số lượng lớn hơn chưa đo lường được vì chưa có hệ thống đủ lớn để đo lường).

- Tính bảo mật và an toàn: Vì là nguồn mở nên không có cam kết khi cài đặt, và mã code không kiểm soát được, nên đã đặt vào những vùng dữ liệu không quá quan trọng đạt kết quả cảnh báo cao.

- Sự hài lòng: giao diện quản lý dễ dùng, thuận tiện trong cấu hình và quản trị.

(6) Phân quyền truy cập dữ liệu trên máy chủ File Server

Để tăng sự an toàn và bảo mật trong lưu trữ dữ liệu em sử dụng máy chủ CentOS tạo thư mục và phân quyền, đồng thời kết hợp với Qouta để giới hạn dung lượng sử dụng hoặc lưu trữ số file của người dùng như sau:

Bước 1: Thực hiện tạo một thư mục có tên data

[root@victs ~]# mkdir /Data

Bước 2: mount thư mục data vào ỗ đĩa vừa tạo

[root@victs ~]# mount /dev/sdb1 /Data

Bước 3: sửa file fstab để thiết lập cố định đường Mount

[root@victs ~]# vi /etc/fstab

Edit file vi fstab:

/dev/sdb1 /Data ext4 defaults,usrquota,grpquota 0 0

Bước 4: mount lại cho thư mục nhận chức năng quota

[root@victs ~]# mount -o remount /Data

Tiếp tục: (bản 6.5 phải cài thêm quota: yum install quota)

[root@victs ~] #chcon --reference=/var /Data (phải có lệnh này. Nếu không thực hiện quotacheck trên 6.5 sẽ bị lỗi)

[root@victs ~]#quotacheck -mcug /Data

[root@victs ~]# ls -l /Data (để xem thư mục data đã có quota chưa).

Bước 5: phân quyền cho thư mục data

[root@victs ~]# chmod 755 /Data

Bước 6: tạo 2 user anln và jenln kèm pass để test chức năng và các group

[root@victs ~]# useradd anln

[root@victs ~]# useradd jenln

[root@victs ~]# password anln

[root@victs ~]# password jenln

[root@victs ~]# groupadd IT

[root@victs ~]# groupadd Sale

[root@victs ~]# usermod -g IT anln

[root@victs ~]# usermod -g Sale jenln

Bước 7: Gán group vào thư mục và phân quyền truy cập để test

[root@victs ~]# mkdir /Data/IT

[root@victs ~]# mkdir /Data/Sale

[root@victs ~]# chgrp IT /Data/IT

[root@victs ~]# chgrp Sale /Data/Sale

[root@victs ~]# chmod 070 /Data/IT

[root@victs ~]# chmod 070 /Data/Sale

Bước 8: cấp hạn ngạch về lượng file cho user jenln (có thể làm với Group)

[root@victs ~]# edquota -u jenln

Disk quotas for user jenln (uid 501):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/sdb1	0	0	0	0	3	5

Chú ý đơn vị quy đổi:

bit: 0 1: 1Byte=8 bit, 1KB=1024 Byte, 1MB=1024 KB, 1GB=1024M

1GB=1000x1000x1000 Byte

2000 = 2MB vì nó tính theo KB

Bước 9: khởi động quota

[root@victs ~]# quotaon -avug

/dev/sdb1 [/Data]: group quotas turned on

/dev/sdb1 [/Data]: user quotas turned on

Bước 10: Sử dụng WinSCP kiểm tra dung lượng

Bước 11: Xem thông tin về quota

$ quota -u nam # user nam

$ quota -g staff # nhóm staff

Để thống kê thông tin quota về các nhóm và user bạn dùng

theo người dùng$ repquota -au

theo nhóm $ repquota -ag

tất cả $ repquota -agu

Đánh giá giải pháp dựa trên kết quả triển khai:

- Tính chính xác của giải pháp phân quyền trên máy chủ file server: đạt độ chính xác cao, khi phân quyền thì chỉ ai mới vào được phòng ban đó, và dung lượng của người dùng cũng chỉ lưu trữ đúng như những gì thiết lập từ ban quản trị.

- Tính hiệu quả: hiệu quả cao vì lưu trữ được trên máy chủ Linux, máy chạy không bị treo khi copy file lớn vào và chế độ hoạt động ổn định.

- Tính bảo mật và an toàn: đạt độ an toàn cao khi phân quyền, mọi người không truy cập chéo được của nhau.

- Sự hài lòng: cấu hình thuận tiện, dễ dùng.

(7) Sao lưu dữ liệu trên File Server

Sao lưu trên CentOS

Đối với máy chủ chạy hệ điều hành Linux, trong đó có CentOS ta dùng Snapshort của LVM (Logical Volume Manager)

- Tạo ổ snapshot

#lvcreate -L 1GB -s -n IT-snap /dev/vg-victs/victs1 (vg=vg-victs, lv=victs1)

Các thành phần câu lệnh:

-L 1GB: Đặt dung lượng cho ổ snapshot

-s: Tạo snapshot

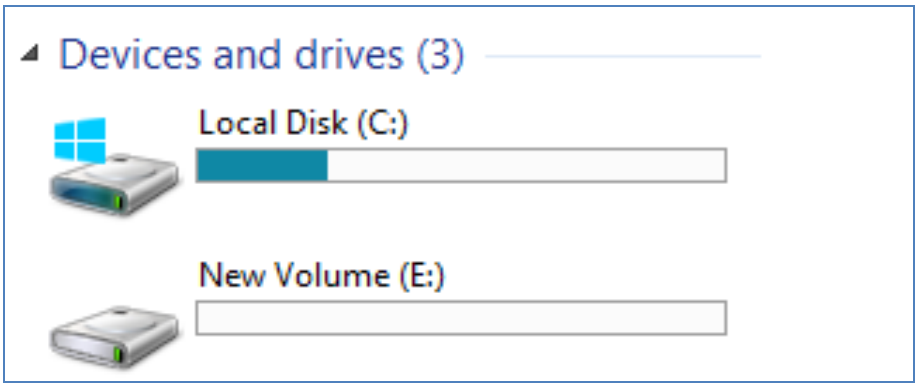
-n: Tạo tên cho snapshot

victs-snap: Tên snapshot

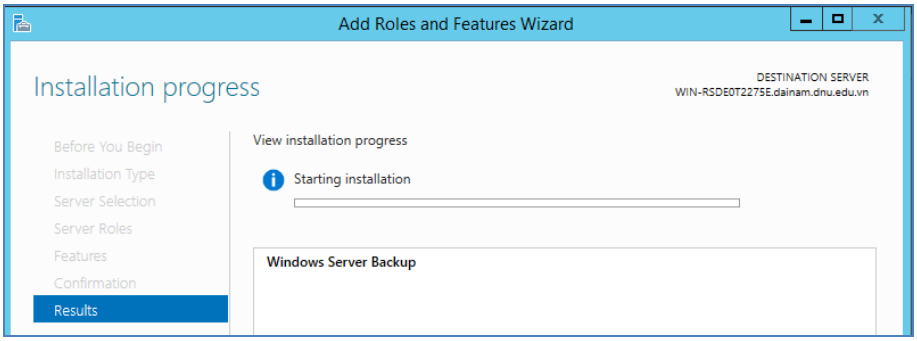
/dev/victs/IT : Volume cần snapshot

Sao lưu trên Windows

Chúng ta cần chuẩn bị một ổ cứng trống để Backup trên Windows Server

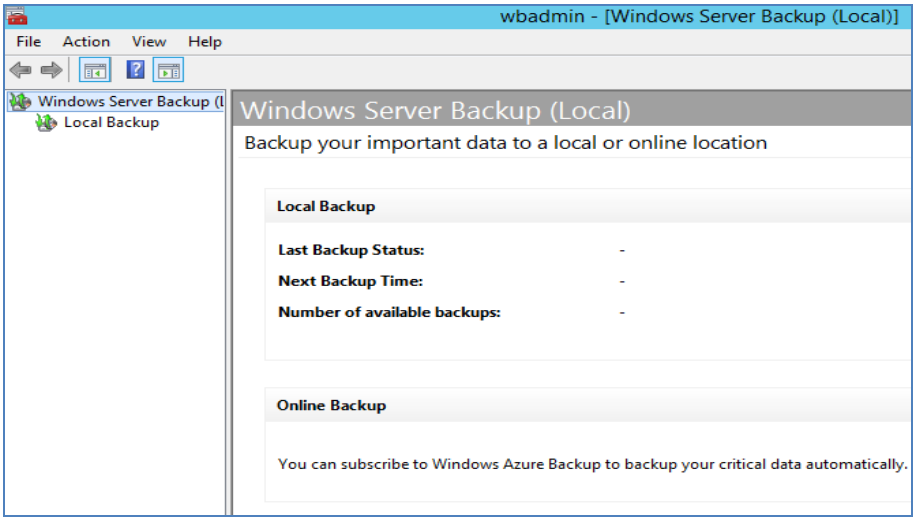


Hình 3.54: Tạo phân vùng mới lưu trữ Backup



Hình 3.55: Cài đặt Window Server Backup

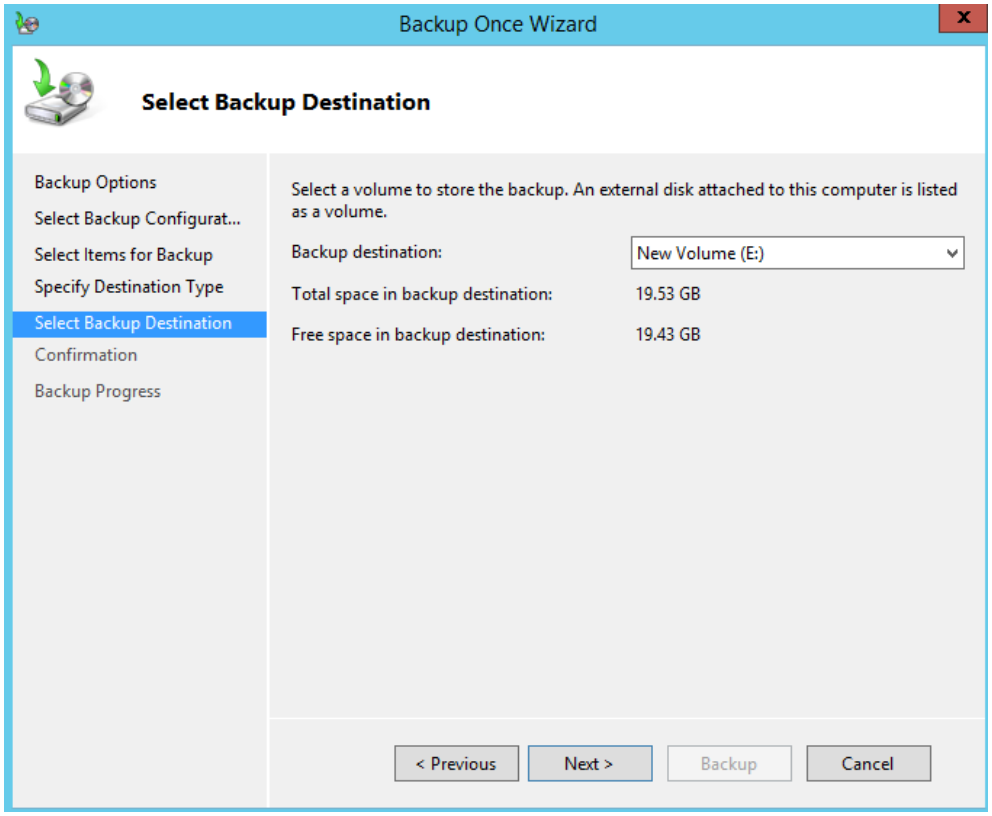
- Sau đó ta khởi động Window Server Backup



Hình 3.56: Giao diện Window Server Backup

- Ta chọn Backup Once, trong này có 2 lựa chọn nhưng sẽ chọn Custom để Backup Folder Data có dữ liệu.

- Sau đó chọn nơi lưu trữ rồi chọn Backup



Hình 3.57: Chọn ổ đĩa lưu trữ Backup

3.3.2 Sau khi thử nghiệm ta có kết quả

Những kết quả thử nghiệm đều cho kết quả khả quan, ổn định và đáp ứng được các yêu cầu bảo mật cho máy chủ ảo cũng như hạ tầng ảo hóa.

Các giải pháp đã cài đặt thử nghiệm có thể đáp ứng cho hệ thống máy chủ ảo hóa tại Viện Khoa học công nghệ sáng tạo Việt Nam và đáp ứng được những nhu cầu trong quá trình vận hành và quản lý tại Viện.

3.4 Kết luận chương 3

Chương 3 của luận văn đã khảo sát mạng nội bộ tại Viện Khoa học công nghệ sáng tạo Việt Nam, các vấn đề nảy sinh trong quá trình sử dụng và các yêu cầu trong bảo mật hệ thống may chủ ảo nhằm đáp ứng nhu cầu của Viện Khoa học công nghệ sáng tạo Việt Nam.

Luận văn cũng đề xuất giải pháp bảo mật máy chủ ảo trong hệ thống ảo hóa và ứng dụng tại Viện Khoa học công nghệ sáng tạo Việt Nam. Qua kết quả từ thử nghiệm hoàn toàn phù hợp với những yêu cầu đặt ra từ ban đầu.

KẾT LUẬN

Với mục tiêu nghiên cứu, áp dụng bảo mật máy chủ ảo trong hệ thống ảo hóa và ứng dụng tại Viện Khoa học công nghệ sáng tạo Việt Nam, luận văn dự kiến đạt được một số kết quả sau đây:

- Tổng quan công nghệ ảo hóa và yêu cầu bảo mật máy chủ ảo.
- Nghiên cứu các giải pháp bảo mật máy chủ ảo trong hệ thống ảo hóa
- Đề xuất giải pháp bảo mật máy chủ ảo trong hệ thống ảo hóa tại Viện khoa học công nghệ sáng tạo Việt Nam

Hướng phát triển tiếp theo:

Học viên sẽ tiếp tục nghiên cứu, hoàn thiện, tối ưu giải pháp hơn nữa để có thể bảo mật máy chủ ảo trong hệ thống ảo hóa và ứng dụng tại Viện Khoa học công nghệ sáng tạo Việt Nam: ở mức cao. Học viên sẽ nghiên cứu thêm công nghệ trí tuệ nhân tạo (AI) để áp dụng vào viêc phát hiện các hành vi tấn công.

IV. DANH MỤC TÀI LIỆU THAM KHẢO

Tài liệu trong nước

[1] Hoàng Xuân Dậu (2007) - *Bài giảng an toàn bảo mật hệ thống thông tin*. Học viện Công nghệ Bưu chính Viễn thông

[2] PGS.TSKH. Hoàng Đăng Hải (2018) - *Quản lý an toàn thông tin - Học viện Công nghệ Bưu chính Viễn thông.* Nhà xuất bản Khoa học Kỹ thuật

[3] Trần Công Cẩn (2019) – *Mô phỏng mạng máy tính Trường Đại học Khánh Hòa* – Trường Đại học Khánh Hòa

[4] Phương Minh Nam (2010) - *Nguy cơ mất an ninh, an toàn thông tin, dữ liệu và một số giải pháp khắc phục* – Bộ Công An

[5] Trần Văn Khá (2008) – *Firewall trong Linux bằng Iptables*

Tài liệu ngước ngoài

[6] Arne Mikalsen and Per Borgesen (2002) - *Local Area Network Management - Design n Security.* University College Norway

[7] Certified Ethical Hacker – Ec Council

[8] Ebook - VMware vSphere 5 Install, Configure, Manage

[9] Ebook - Sybex.Mastering.VMware.vSphere.5.Sep.2011

[10] Ebook - Securing VMware ESX servers

[11] Documentation for Ussuri (May 2020) - https://docs.openstack.org

[12] Certified Information System Security Professional – Microsoft

[13] Cisco Certified Network Associate – Cisco Academy

[14] David Miller et al (2010) Security Information and Event Management

[15] Eliud Ir. Eliud Aganze (2014) - *Design Implementation And Management Of* Secured LAN MSc. Jomokenyatta University of Agriculture And Technology.

[16] Gert De Laet, Gert Schauwers (2004) - *Network Security Fundamentals.* Publisher Cisco Press.

[17] Helling (2015) - *Home Network Security.* Eindhoven University of

Techonogy.

[18] IETF RFC 1701: Generic Routing Encapsulation (GRE)

[19] IETF RFC 2637: Point - to - Point Tunneling Protocol (PPTP)

[20] IETF RFC 2661: Layer Two Tunnuling Protocol (L2TP)

[21] Jan Vykopal (2008) - *Security Analysis of a Computer Network.* Masaryk University Faculty of Informatics.

[22] Kaiyuan Yang (2011) - *Bachelor's Thesis.* Abstract Turku University of Applied Sciences.

[23] Kevin Wey Kaye Tham (2006) - *Dev Security Service For Network Architectures*. PhD Quyeesland University of Technology.

[24] Overview of Virtual Private Networks and IPSec Technologies - Cisco System.

[25] R.C.Sreijl (2000) - Analysis of Managed Virtual Private Network

[26] Tamirat Atsemegiorgis (20130 - *Building a Secure Local Area Network.* Helsinki Metropolia University of Applied Sciences.

Tài liệu từ Internet:

[27] http://www.cisco.com/go/vpn

[28] http://www.lpi.org/

[29] http://www.vjst.vn/vn/tin-tuc/2653/big-data-va-ung-dung-trong-bao-mat-thong-tin.aspx

[30] https://ictnews.vietnamnet.vn/cntt/bao-mat/nua-dau-nam-2019-so-cuoc-tan-cong-mang-vao-cac-he-thong-thong-tin-viet-nam-tiep-tuc-giam-184932.

[31] https://securitydaily.net/splunk-cong-cu-toan-nang-cho-cac-chuyen-gia-giam-sat-an-ninh-mang/

[32] https://trendmicro.ctydtp.vn/10-vu-tan-cong-internet-lon-nhat-lich-su.html

[33] https://vnetwork.vn/vi/news/10-thong-ke-ve-an-ninh-mang-2019

[34] https://www.elastic.co/elk-stack/

[35] https://www.elastic.co/products

[36] https://www.snort.org/