HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 02

TRIỂN KHAI TƯỜNG LỬA CHECKPOINT

Người xây dựng bài thực hành:

ThS. Phạm Minh Thuấn

HÀ NỘI, 2015

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Triển khai tường lửa CheckPoint
Module: An toàn mạng máy tính
Số lượng sinh viên cùng thực hiện: 01
Địa điểm thực hành: Phòng máy
Yêu cầu:

- Yêu cầu phần cứng:
  + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 3.0 GHz, RAM 4GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
  + Hệ điều hành Windows XP/7/8
  + VMware Worstation 11.0 trở lên
- Công cụ thực hành:
  + Máy ảo Vmware Windows 7.
  + Máy ảo CentOS 6.5
  + Bộ cài đặt Firewall CheckPoint R75
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

- ISO Firewall CheckPoint R75 cho Linux
- ISO Firewall CheckPoint R75 cho Windows
- ISO CentOS 6.5
- Phần mềm SecureCRT

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

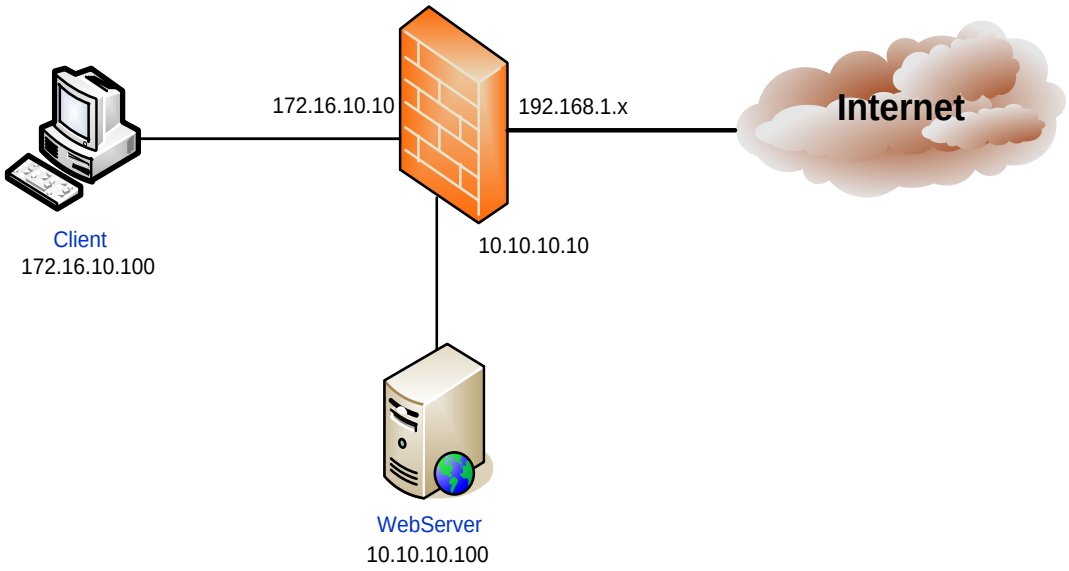
PHẦN 1. THỰC HÀNH TRIỂN KHAI TƯỜNG LỬA CHECK POINT TRÊN HĐH SECURE PLATFORM

Check Point Software Technologies (NASDAQ - CHKP) là một trong những công ty hàng đầu thế giới về an toàn an ninh Internet. Check Point được biết đến với công nghệ nổi tiếng Stateful Inspection – một trong những công nghệ tường lửa phổ biến nhất hiện nay được phát minh và đăng ký bản quyền năm 1994 cùng với nền tảng OPSEC (Open Platform for Security) đã góp phần tạo thêm sức mạnh về độ an toàn cũng như các tính năng trên các sản phẩm tường lửa của hãng.

Trong bài thực hành này, sinh viên sẽ được tiếp cận với tường lửa Check Point triển khai trên hệ điều hành Secure Platform nhân Linux để có thể triển khai đảm bảo an toàn cho hệ thống mạng.

1.1. Mô hình triển khai

Sinh viên cần chuẩn bị các máy ảo để xây dựng mô hình mạng theo sơ đồ như sau:



Trong đó:

❖ **Máy ảo 1 (Firewall CheckPoint):**

- Cài đặt Firewall CheckPoint theo mô hình StandAlone trên nền tảng SecurePlatform
- Sử dụng 03 giao diện mạng:
  + Địa chỉ IP: 192.168.1.x. Bridge
  + Địa chỉ IP: 10.10.10.10. VMNet2
  + Địa chỉ IP: 172.16.10.10. VMNet3

❖ **Máy ảo 2 (WebServer):**

- Cài đặt hệ điều hành Windows Server 2003 SP2

- Cài đặt dịch vụ WebServer
- Tạo 1 Website đơn giản để có thể truy cập tới WebServer
- Địa chỉ IP: 10.10.10.100

❖ **Máy ảo 3 (Client):**

- Cài đặt hệ điều hành Windows 7
- Cài đặt SmartConsole

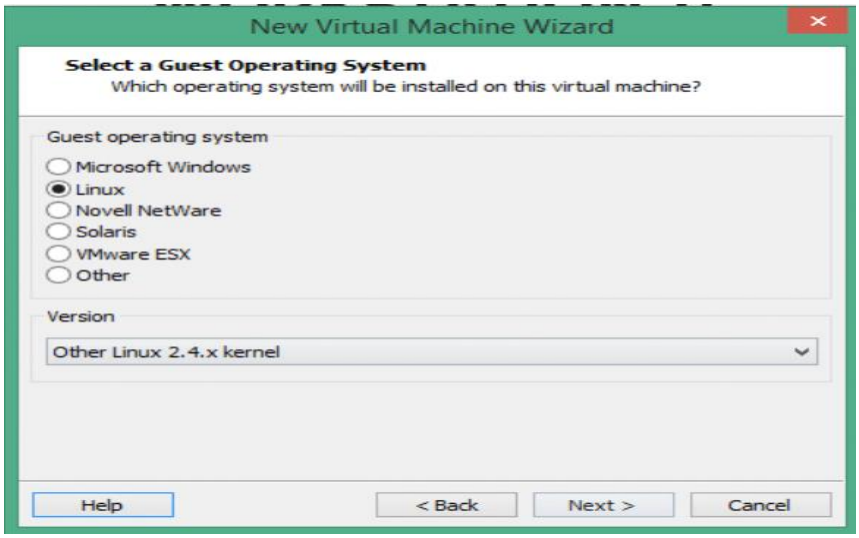
  Địa chỉ IP: 172.16.10.100

1.2. Cài đặt thành phần Security Gateway và Security Management trên HĐH SecurePlatform

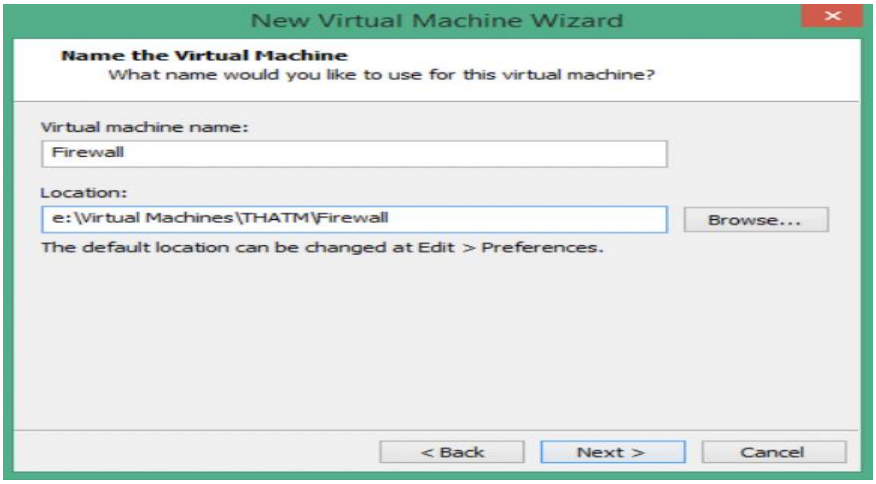
1.2.1. Cài đặt máy ảo tường lửa

Đầu tiên, chọn Creat a New Virtual Machine -> chọn Custom -> Next

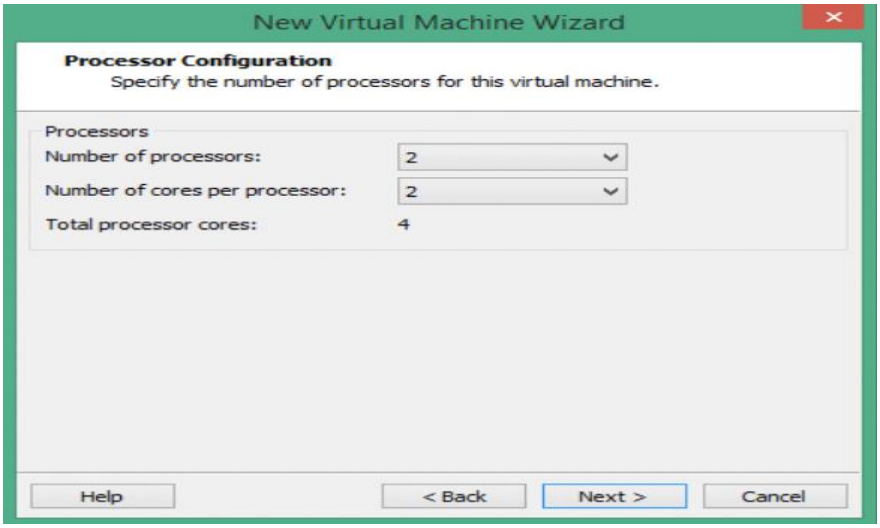
Thực hiện chọn hệ thống Linux như hình dưới -> Next



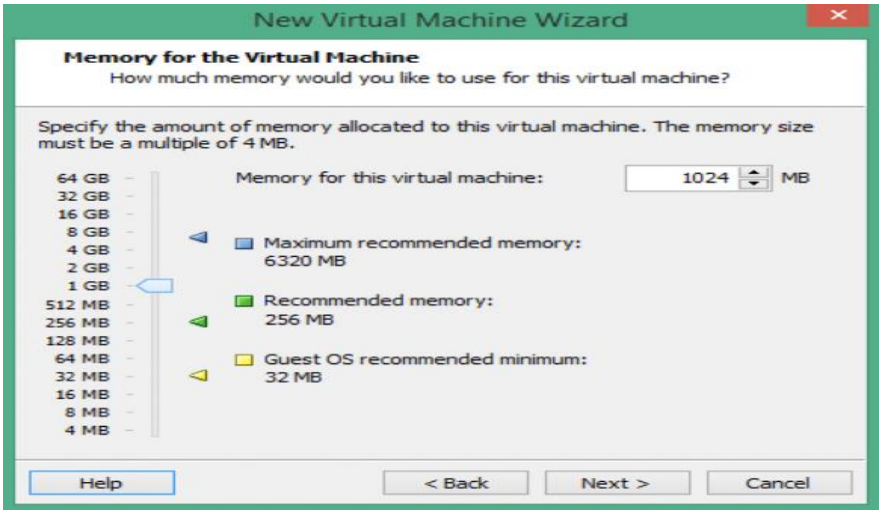
Đặt tên cho firewall và nơi lưu trữ nơi cài đặt firewall -> chọn ok



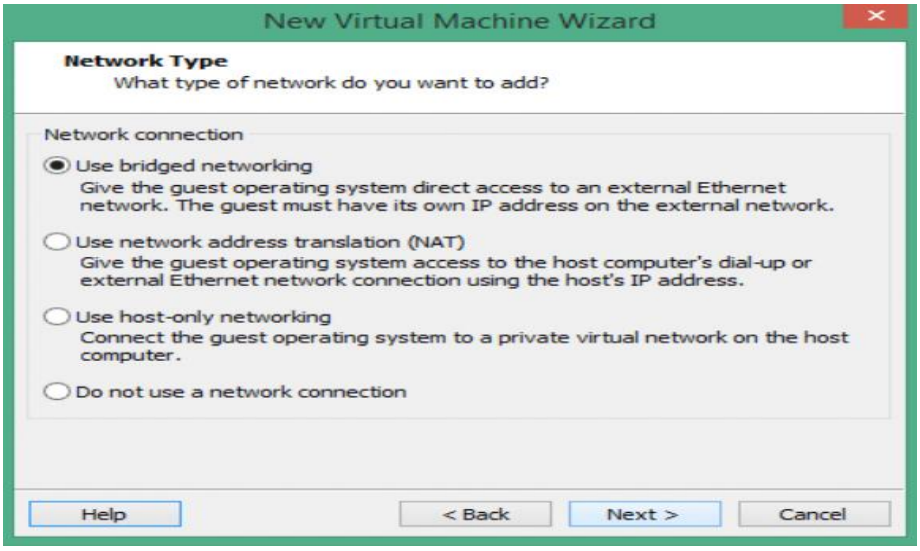
Cài đặt các tiến trình tiếp như hình dưới -> chọn Next



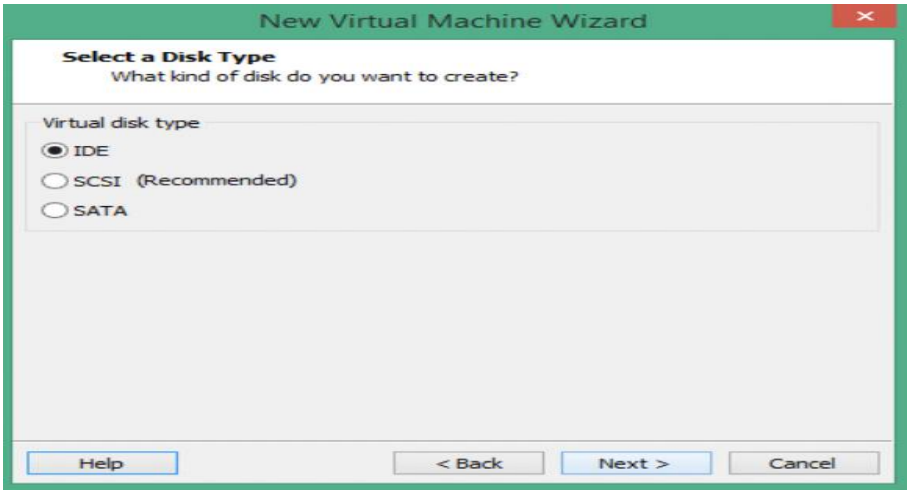
Thiết lập bộ nhớ RAM cho firewall



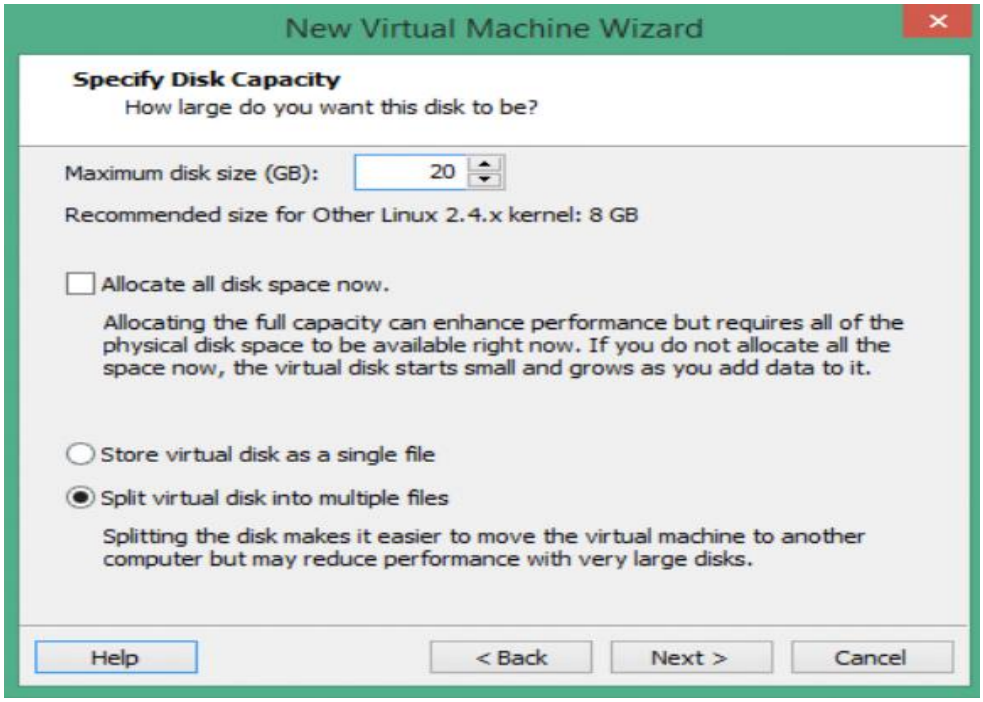
Cài đặt chế độ card mạng cho firewall ->next



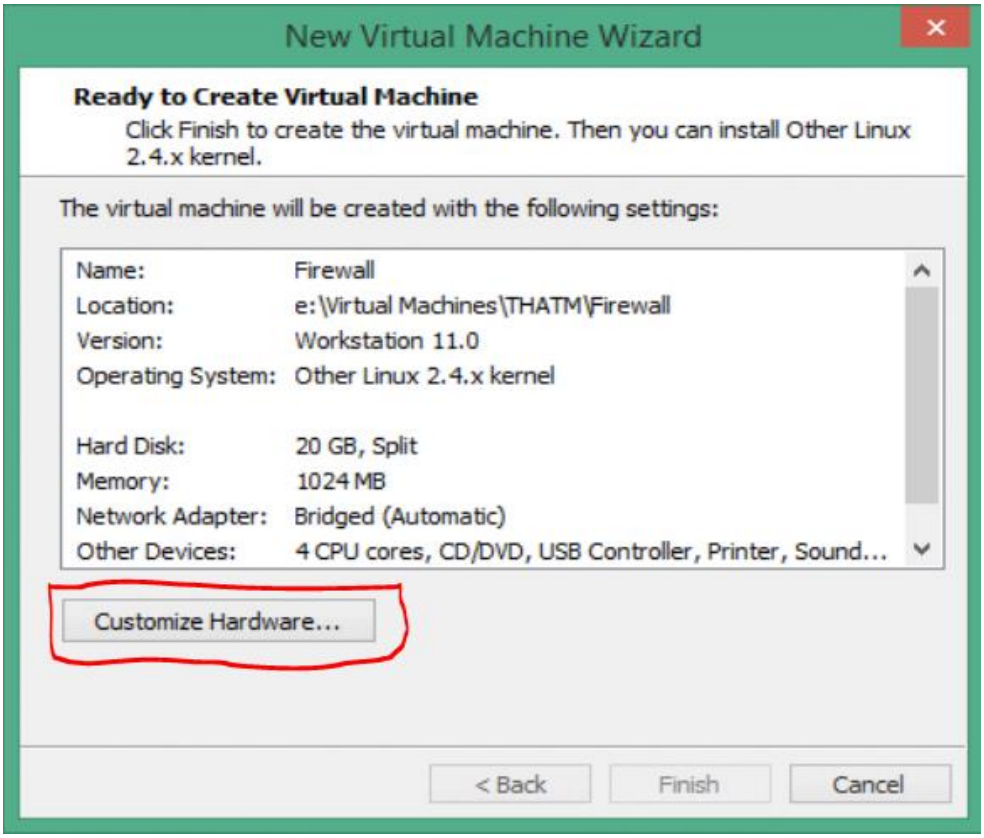
Thiết lập dạng ổ đĩa cài đặt và lưu trữ cho firewall ta chon kiểu IDE.



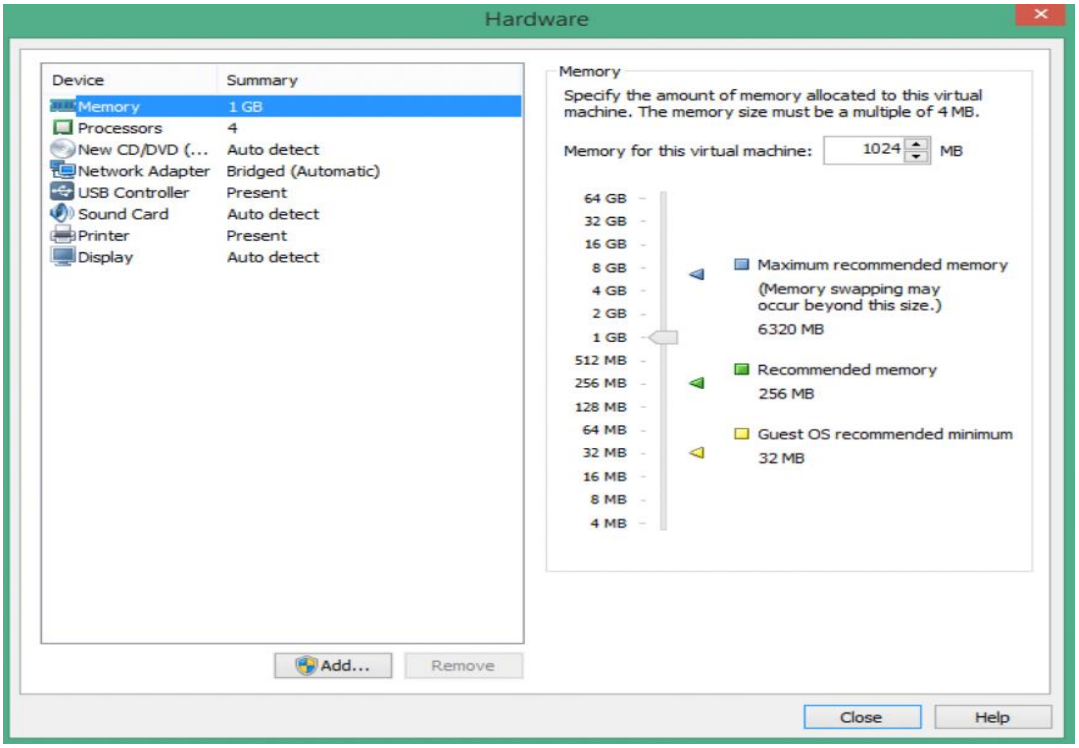
Thiết lập dung lượng ổ cứng cho firewall như hình dưới -> chọn next



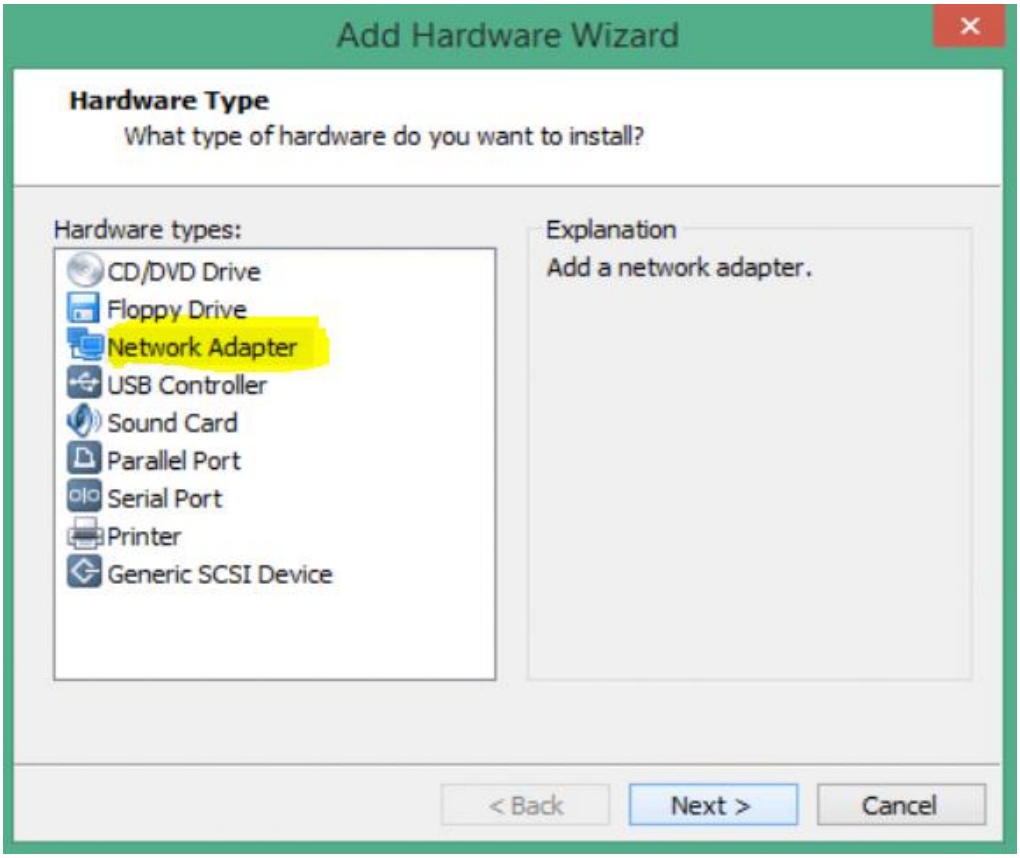
Chọn Customize Hardware để thêm Card mạng ở đây ta cần thêm 3 card mạng theo đúng mô hình.



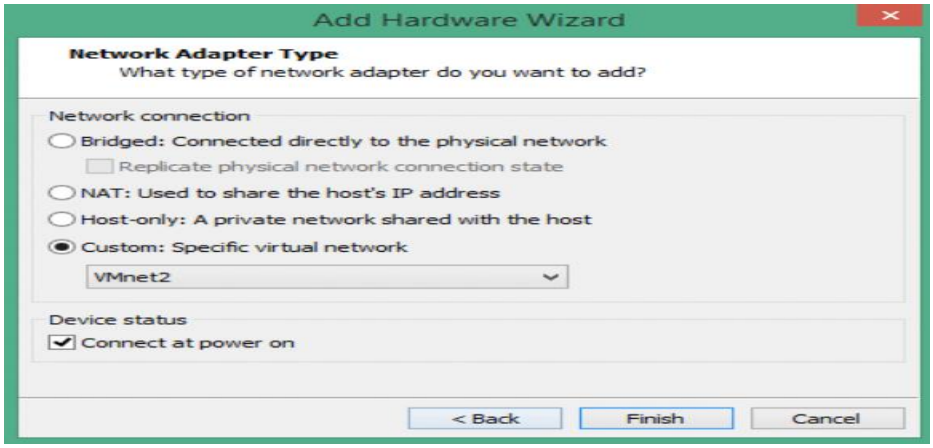
Sau khi chọn Customize Hardware xuất hiện 1 bảng Hardware như hình dưới . Chọn Add.. để tiến hành thêm card mạng cho firewall



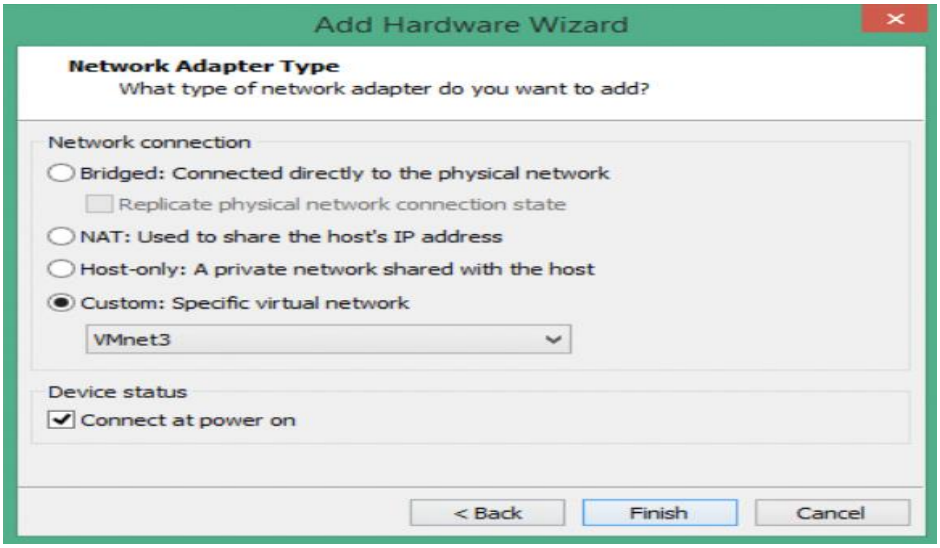
Chọn Network Adapter



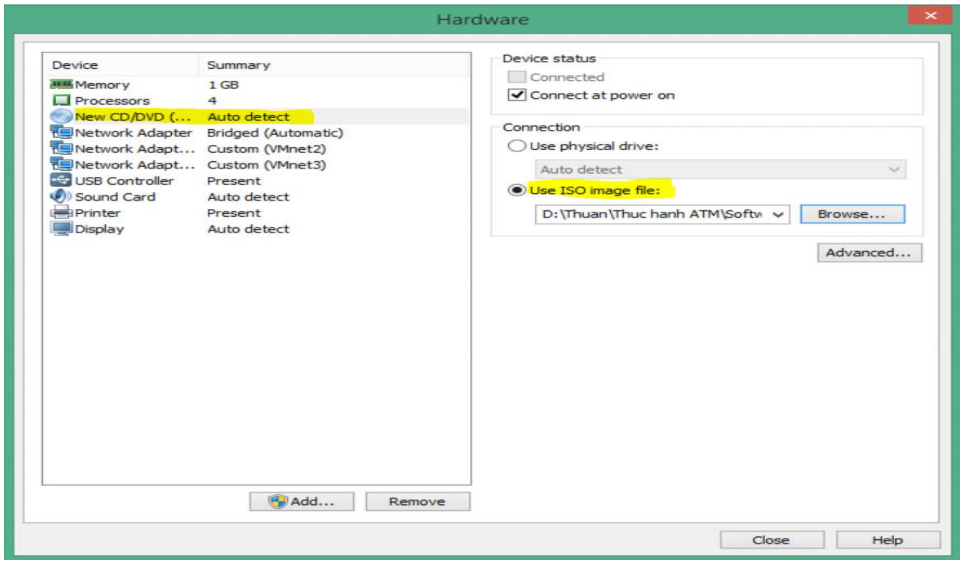
Thực hiện theo hình thêm Card mạng Vmnet2



Thực hiện tương tự để thêm Card mạng Vmnet3

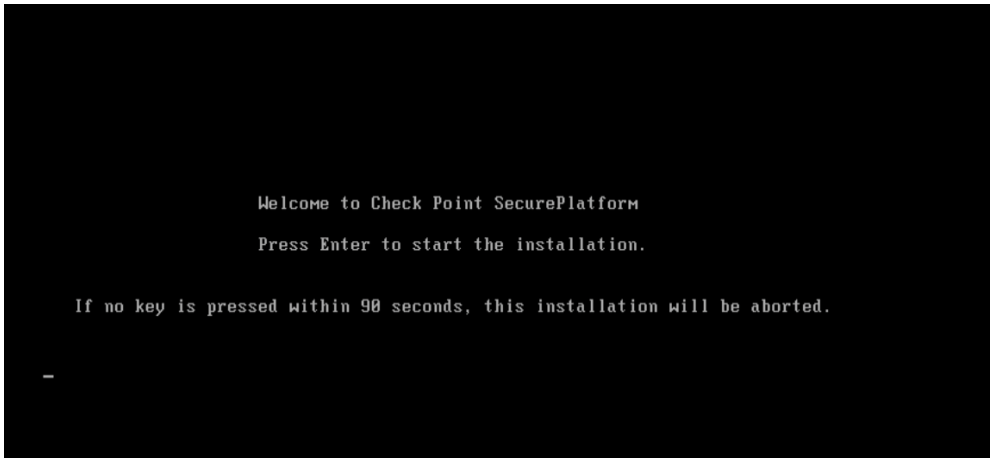


Sau khi thêm Card mạng, chọn New CD/DVD … -> Ấn Browse ở Use ISO image file để thêm file ISO Checkpoint. Sau đó ấn Close -> Finish.



1.2.2. Cài đặt tường lửa

Chọn "Power on this virtual machine" để khởi động Firewall

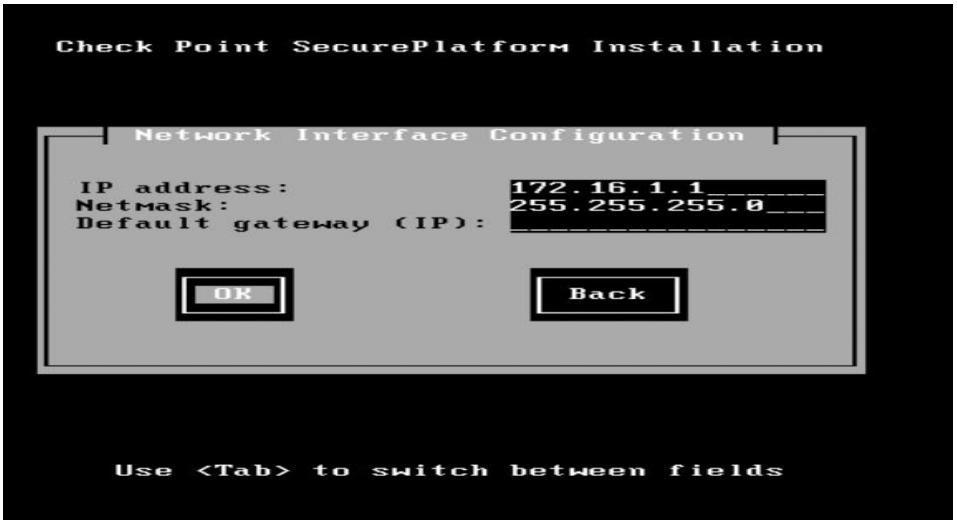


Thực hiện các bước tiếp theo hình chọn OK

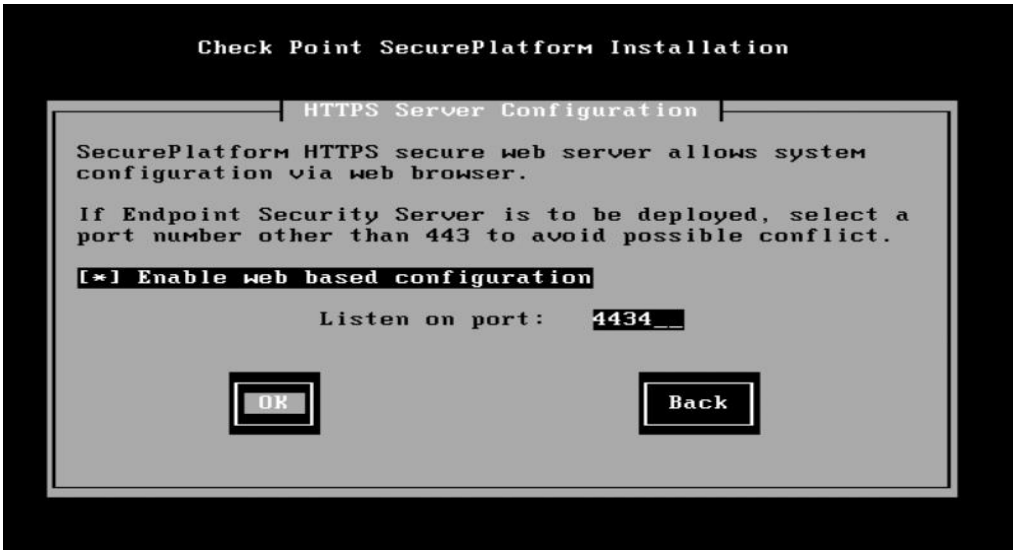
Chọn kiểu bàn phím US chọn OK

Ta tiến hành cấu hình các card mạng eth2 (LAN)

Đặt địa chỉ IP cho card eth2 (mạng LAN)



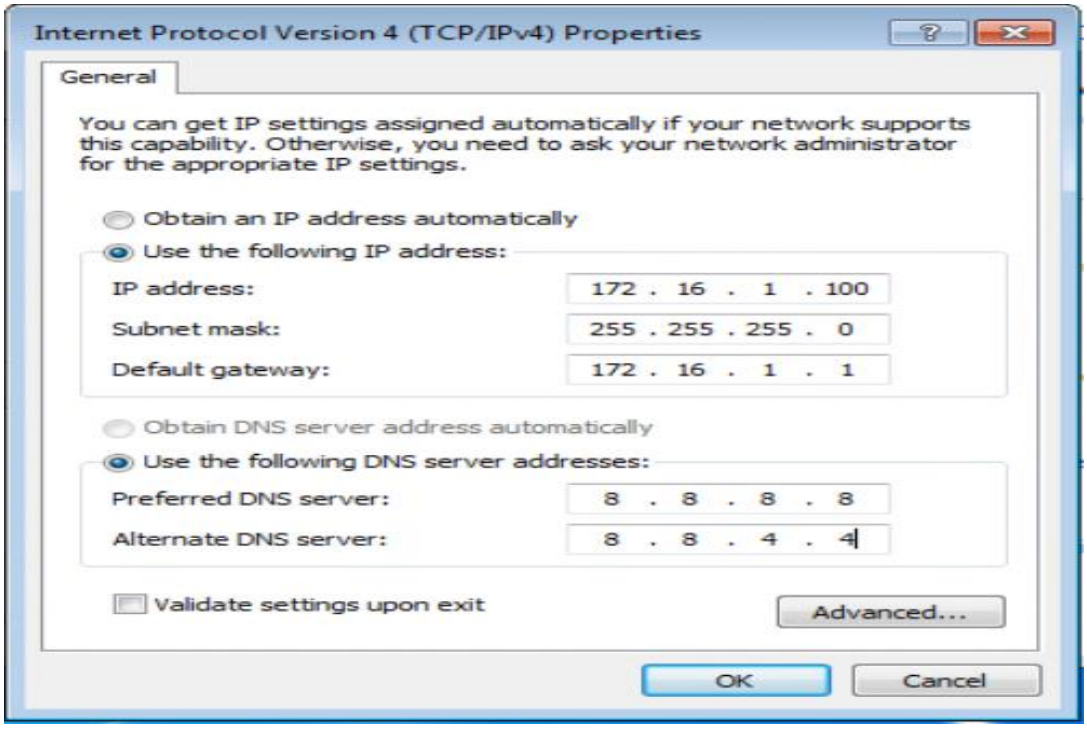
Thay đổi port thành port 4434 -> chọn OK để cài đặt firewall



Khi kết thúc tiến trình cài đặt firewall yêu cầu khởi động lại firewall

Vậy ta đã hoành thành quá trình cài đặt firewall check point. Ta tiến hành bật máy client windows 7 để đăng nhập vào Check Point để cài cấu hình và cài đặt các thông số kĩ thuật.

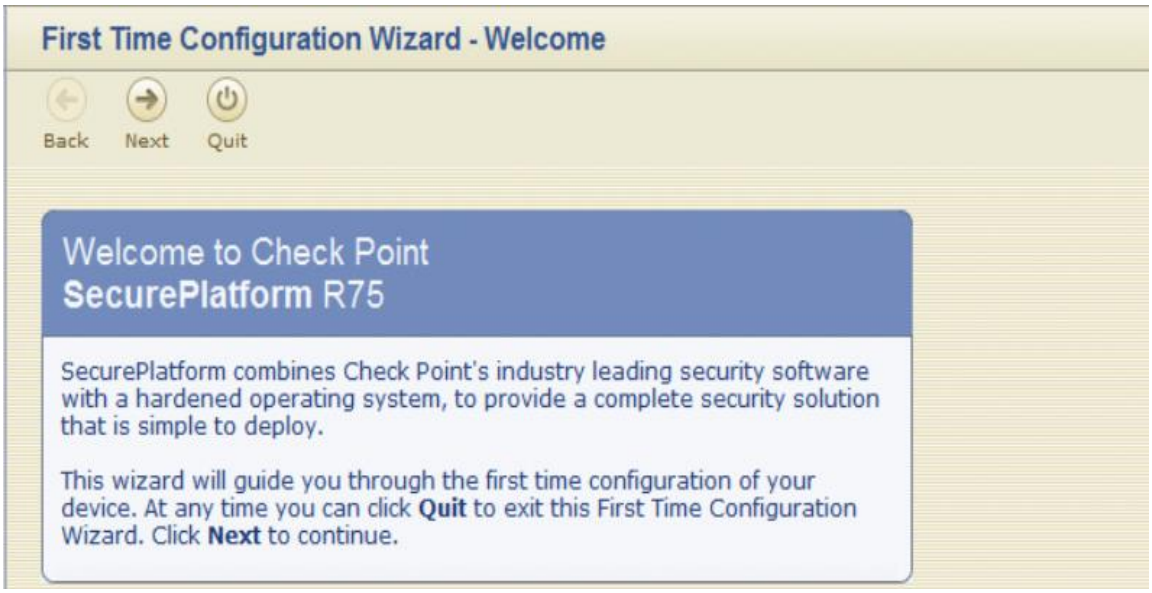
Máy client ở đây ta cài đặt về card mạng vmnet3 và đặt địa chỉ IP trùng với dải ip 172.16.1.1/24 . Ta tiến hành cài đặt như hình sau :



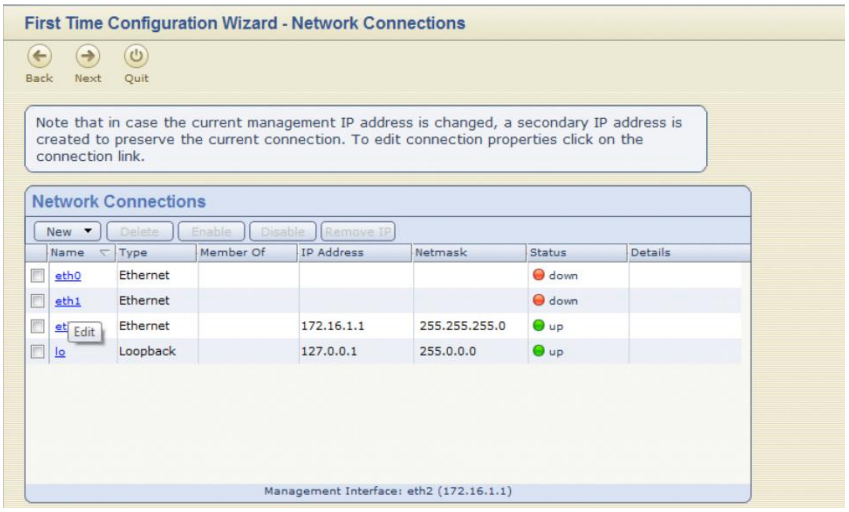
Sau khi đặt địa chỉ ip ta tiến hành truy cập vào web theo địa chỉ "https:// 172.16.1.1:4434" ban đầu khi ta đăng nhập mặc định trình duyệt mặc định chặn ta chọn "continue to this website" -> chọn "I Accept" sẽ xuất hiện hộp thoại đăng nhập sau : username và password ở đây mặc định là "admin : admin"

Lần đăng nhập đầu tiên mặc định sẽ tự động yêu cầu bắt chúng ta đổi mật khẩu username và password . Ta tiến hành nhập username, password mới và tiến hành đăng nhập.

Khi ta đăng nhập sẽ tiến hành các cài đặt thông số như sau : Chọn Next

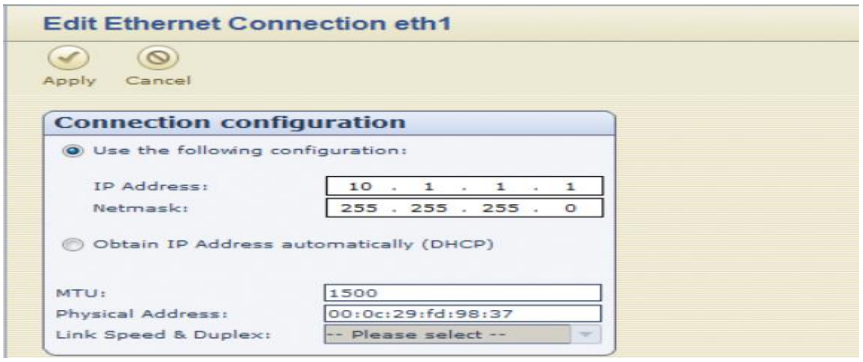


Tiếp đến ta phải cấu hình các giao diện mạng cho firewall có 3 giao diện mạng chúng ta cần cấu hình là eth0, eth1, eth2

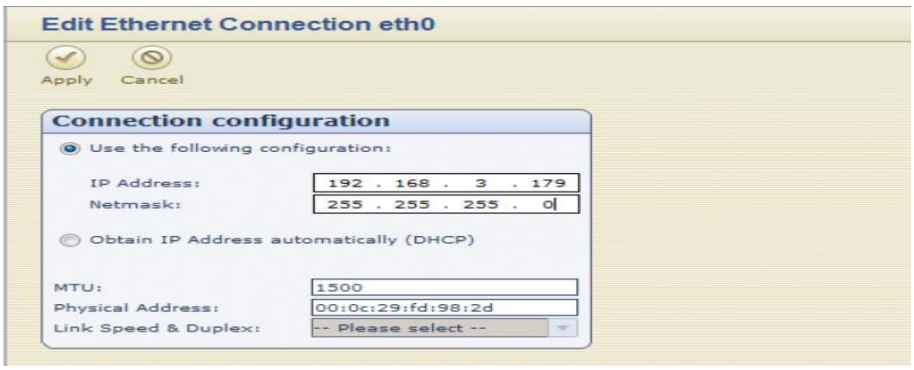


Chọn 1 giao diện mạng ta kích đúp chuột vào để cài đặt các thông số cho từng giao diện mạng một

Với Eth1 tương ứng với Vmnet2 ta hướng card mạng này đến vùng chứa các máy chủ dịch vụ cấu hình các thông số như sau :

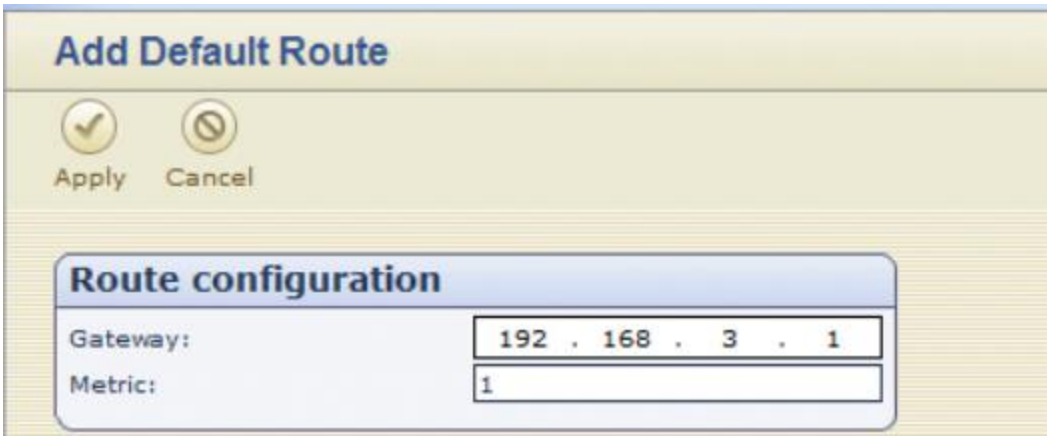


Với eth0 chính là card mạng hướng ra ngoài internet ta cấu hình tùy thuộc vào địa chỉ ip trong mạng LAN trên máy thật của chúng ta sẽ cấu hình cho phù hợp -> Apply để lưu lại



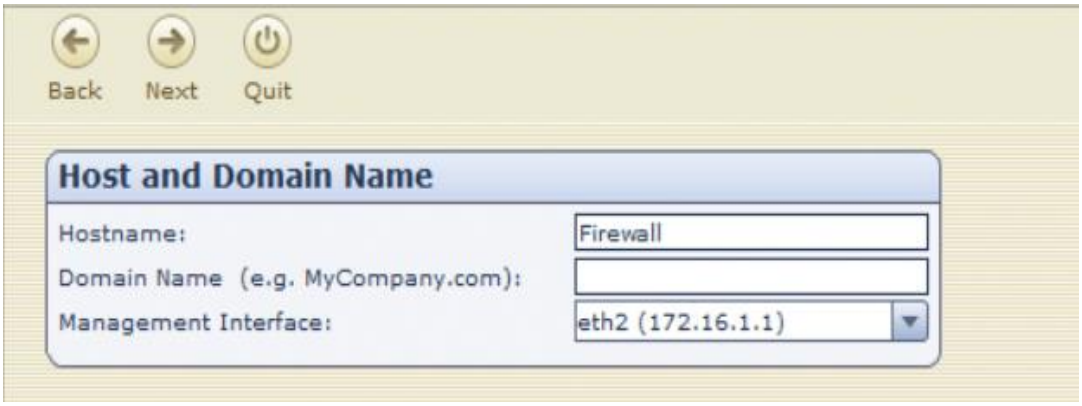
Khi cài đặt xong các card mạng ta chọn Next tiếp tục cài đặt. Tiếp theo chúng ta cần tiến hành cài đặt Routing Table. Mục đích của cài đặt này cho tất cả các kết nối đến các giao diện mạng đều phải đi qua đó.

Chọn Default Route ta cấu hình xong ta chọn -> Apply

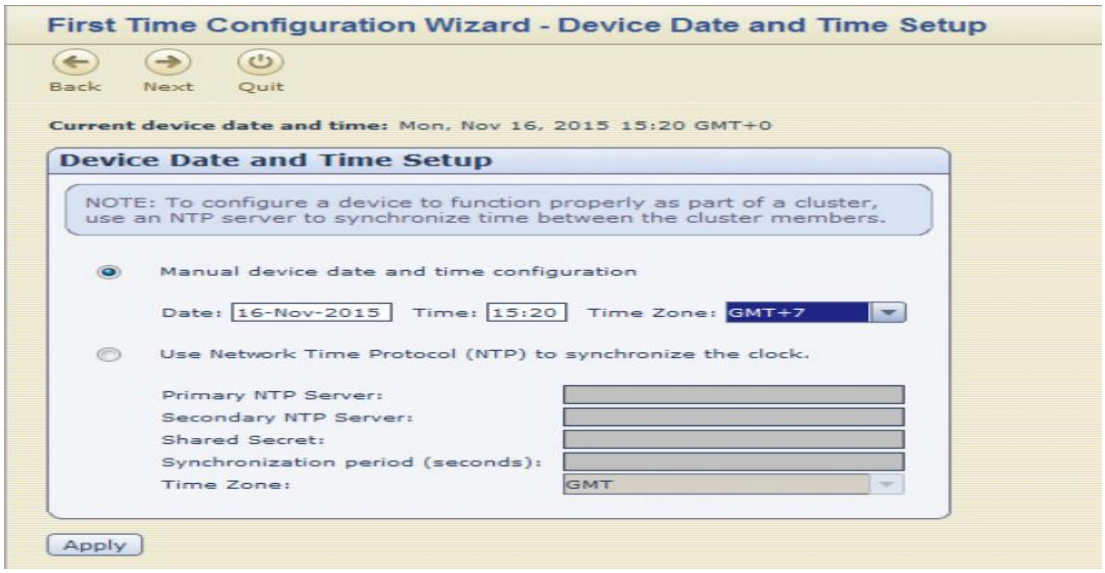


Tiếp theo cấu hình DNS cho firewall như sau. Xong ta chọn Next

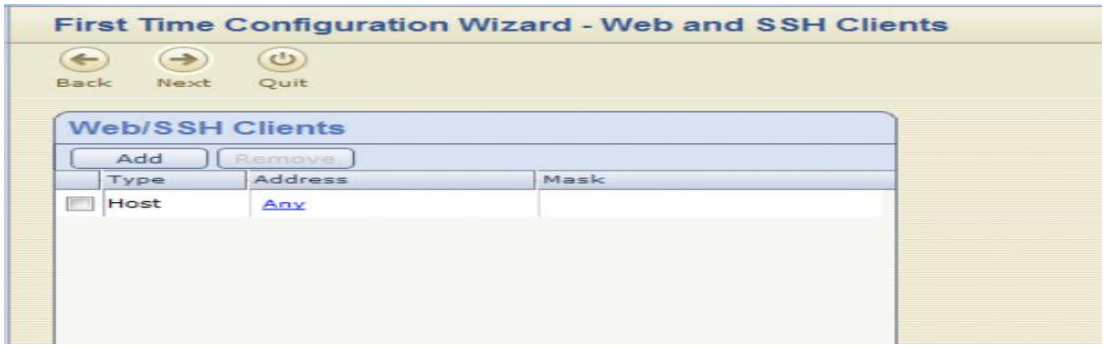
Sau khi cấu hình DNS xong ta tiến hành cài đặt tên cho firewall và giao diện mạng kết nối đến cấu hình firewall.



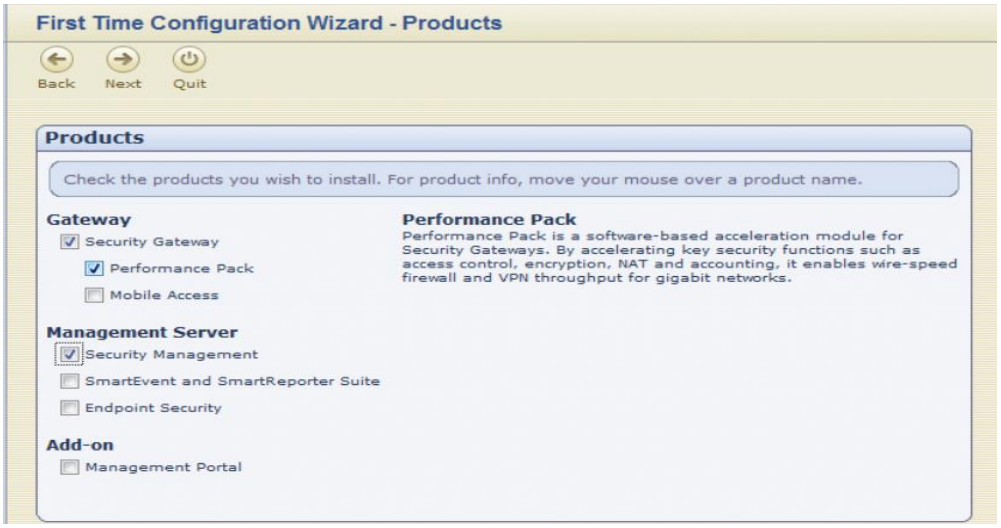
Cài đặt thời gian cho firewall thời gian ở đây ta cần chọn đúng và đồng bộ với thời gian thực trên máy tránh trường hợp xảy ra lỗi khi kết nối ra bên ngoài. Xong ta chọn Next



Cài đặt các máy có thể kết nối đến firewall để cấu hình ta để mặc định ->Next

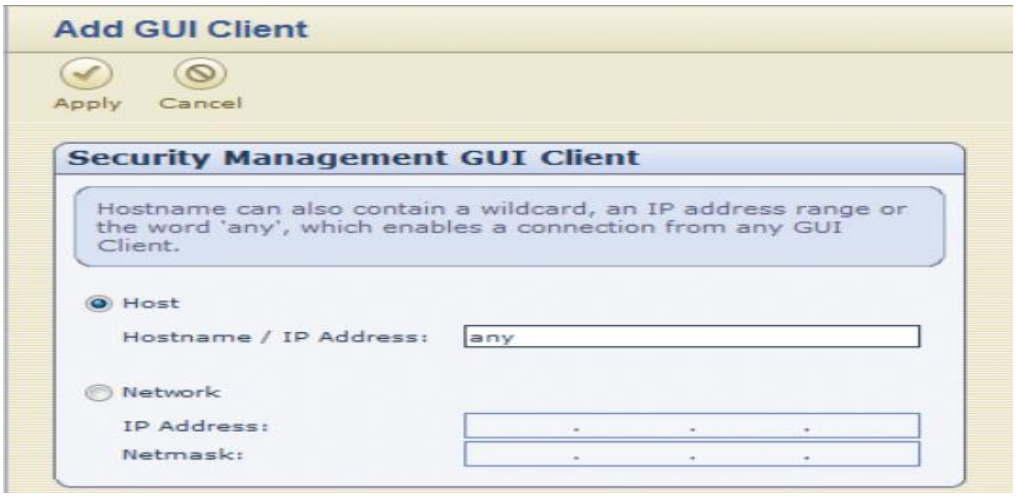


Lựa chọn các thành phần cài đặt cho firewall. Cấu hình như hình sau



Tiếp theo cấu hình Security Management chọn như hình dưới.

Ta cấu hình Security Management GUI client. Ta chọn : add rồi điền các thông số cấu hình như hình sau :

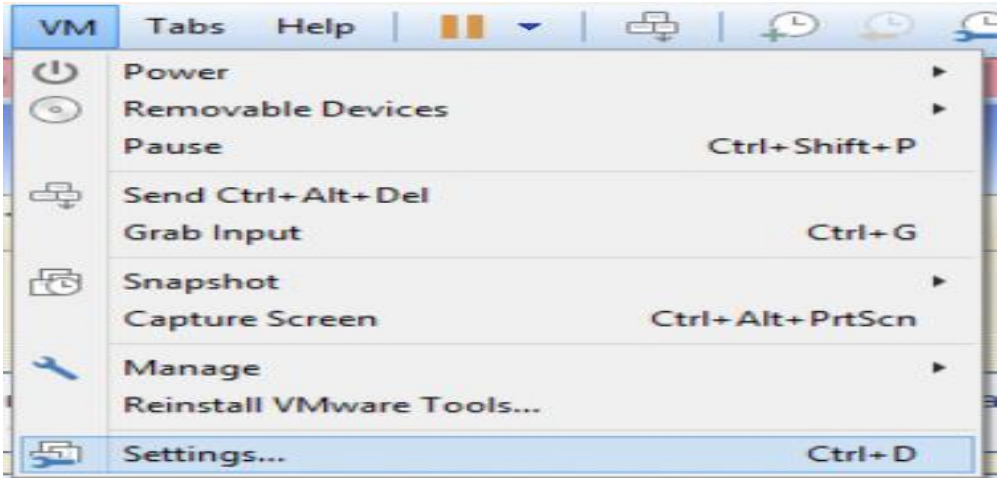


Sau khi cấu hình Security Management GUI client chọn next ,ta cấu hình Security Management Adminitrators ta thêm tài khoản quản trị cho check point . Ta chọn add để thêm tài khoản quản trị vào

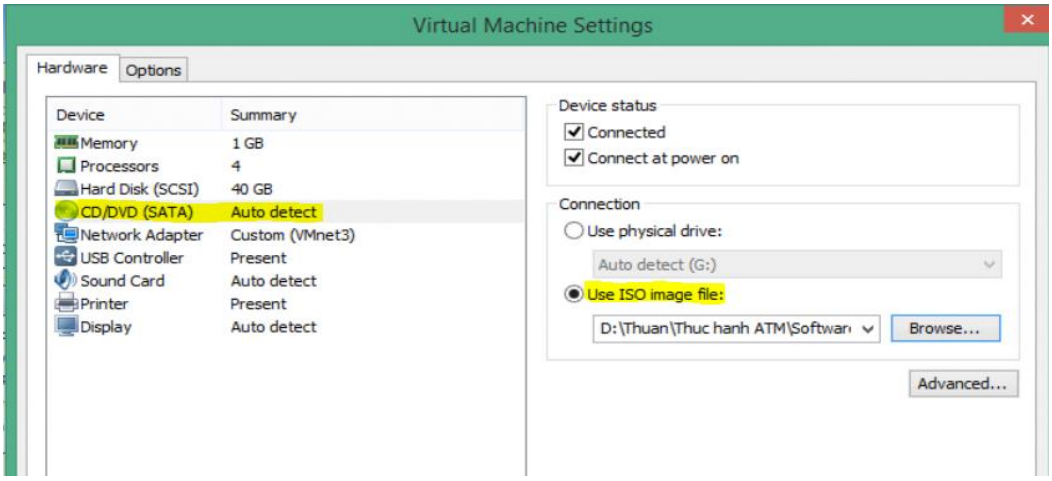
Khi thêm tài khoản quản trị cho firewall ta chọn next là ta đã tiến hành cài đặt xong Check point

1.3. Cài đặt thành phần SmartConsole trên HĐH Windows

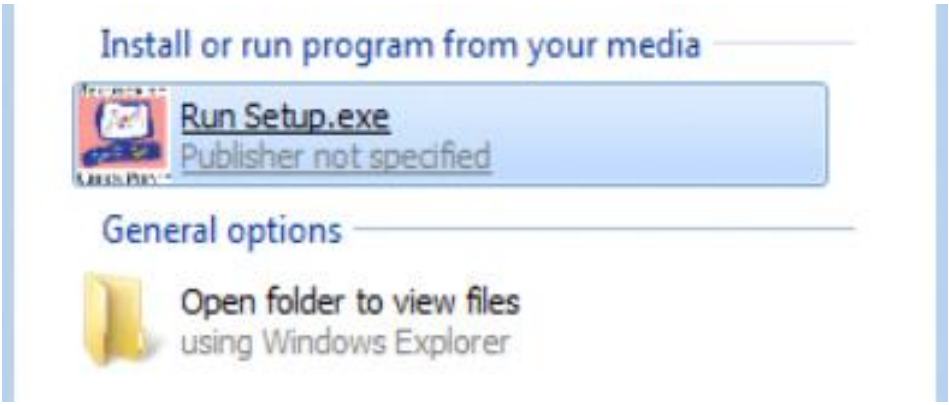
Trên máy client ta tiến hành thêm file iso vào để cài đặt smart console



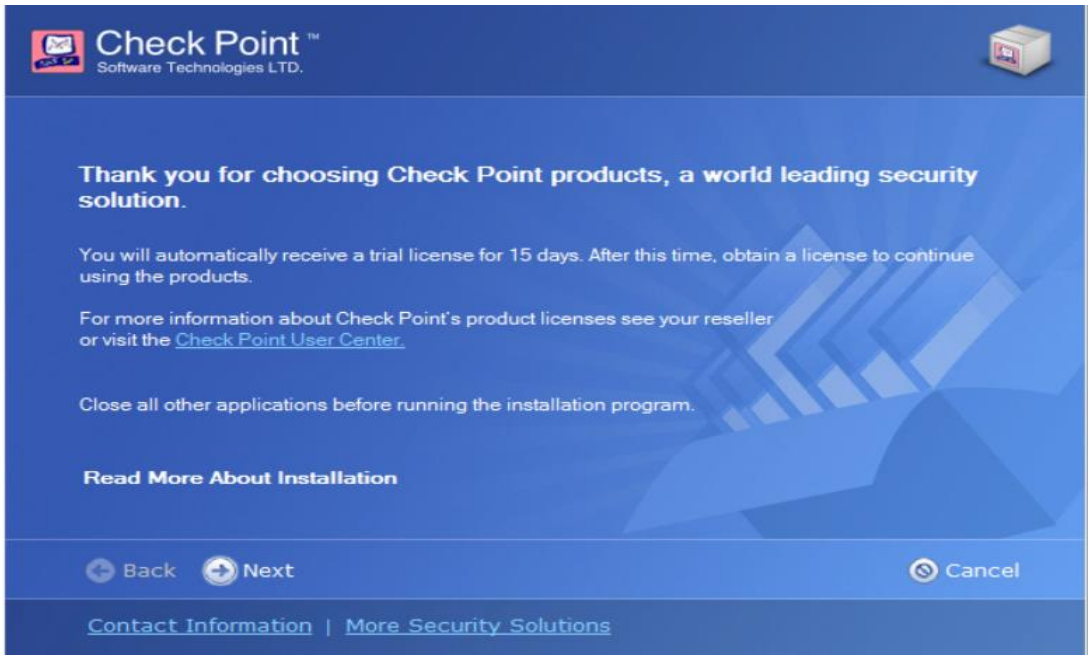
Đưa file iso vào ổ đĩa cd của client như sau:



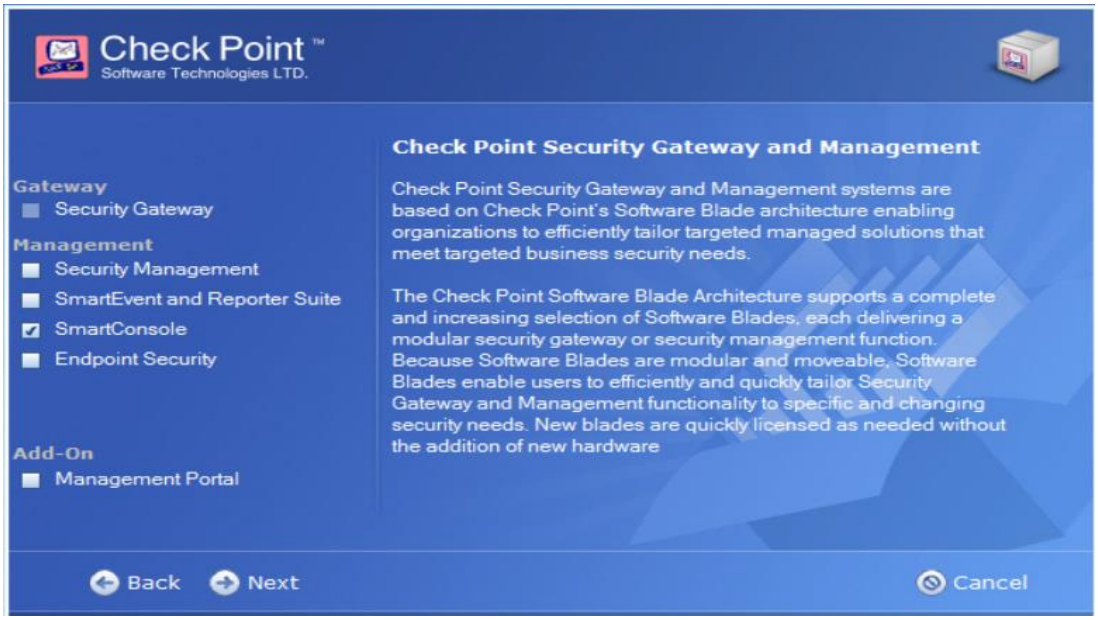
Chạy file cài đặt Smart console



Chọn Next



Tại cài đặt tại phần cài đặt có 2 chế độ ta chọn Custom và ta chỉ chọn lựa SmartConsole

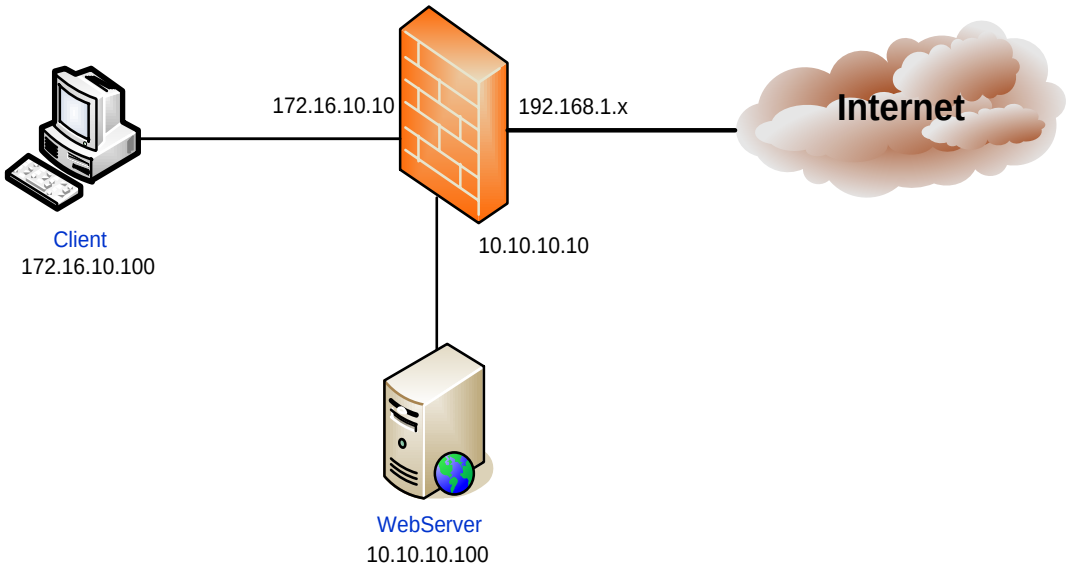


Chọn Next cho đến khi kết thúc quá trình cài đặt.

PHẦN 2. THỰC HÀNH QUẢN TRỊ TƯỜNG LỬA CHECK POINT

2.1. Chuẩn bị

Sinh viên cần chuẩn bị các máy ảo để xây dựng mô hình mạng theo sơ đồ như sau:



Trong đó:

❖ **Máy ảo 1 (Firewall CheckPoint):**

- Cài đặt Firewall CheckPoint theo mô hình StandAlone trên nền tảng SecurePlatform
- Sử dụng 03 giao diện mạng:
  + Địa chỉ IP: 192.168.1.x. Bridge
  + Địa chỉ IP: 10.10.10.10. VMNet2
  + Địa chỉ IP: 172.16.10.10. VMNet3

❖ **Máy ảo 2 (WebServer):**

- Cài đặt hệ điều hành Windows Server 2003 SP2
- Cài đặt dịch vụ WebServer
- Tạo 1 Website đơn giản để có thể truy cập tới WebServer
- Địa chỉ IP: 10.10.10.100

❖ **Máy ảo 3 (Client):**

- Cài đặt hệ điều hành Windows 7
- Cài đặt SmartConsole

Địa chỉ IP: 172.16.10.100

Yêu cầu thực hiện:

- Cấu hình Anti-Spoofing cho Firewall.
- Thiết đặt các luật trên Firewall sao cho:
  + Chặn tất cả các truy cập trái phép vào Firewall.

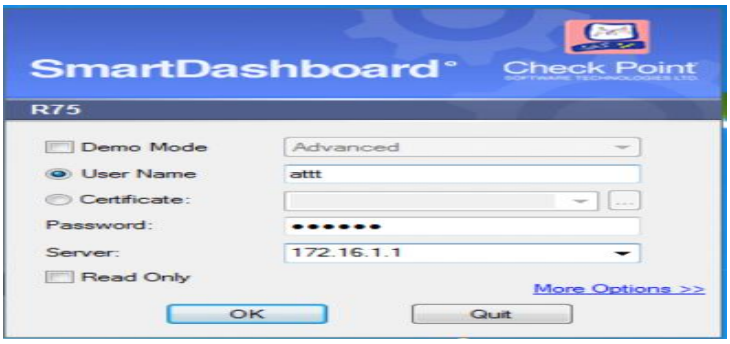
+ Sử dụng NAT quảng bá WebServer ra bên ngoài, cho phép người sử dụng truy cập vào WebServer qua giao thức HTTP và HTTPS, cho phép ping.
+ Cho phép Client được phép truy cập ra Internet nhưng cấm sử dụng Yahoo Messenger và cấm chơi game online (port>1024).
+ Chỉ có Client có địa chỉ IP 172.16.10.100 mới được phép truy cập vào vùng 10.10.10.0/24. Còn lại các máy khác nằm trong dải 172.16.10.0/24 đều không được phép truy cập vào vùng mạng trên.
+ Tất các các truy cập khác đều bị cấm.

2.2. Xây dựng chính sách trên tường lửa

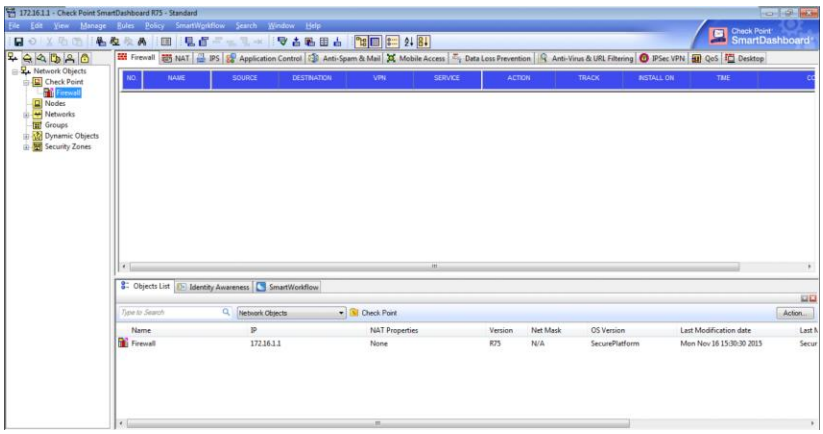
2.2.1. Kết nối tới tường lửa

Từ máy Client tiến hành đăng nhập thông qua thành phần SmartConsole vào thành phần Security Management trên tường lửa Checkpoint

+ User Name: tài khoản quản trị của Security Management (tài khoản này khác so với tài khoản sử dụng khi đăng nhập vào HĐH SecurePlatform)
+ Password: mật khẩu tương ứng với tên đăng nhập
+ Server: Địa chỉ máy chủ Security Management (trong mô hình StandAlone chính là địa chỉ của tường lửa)

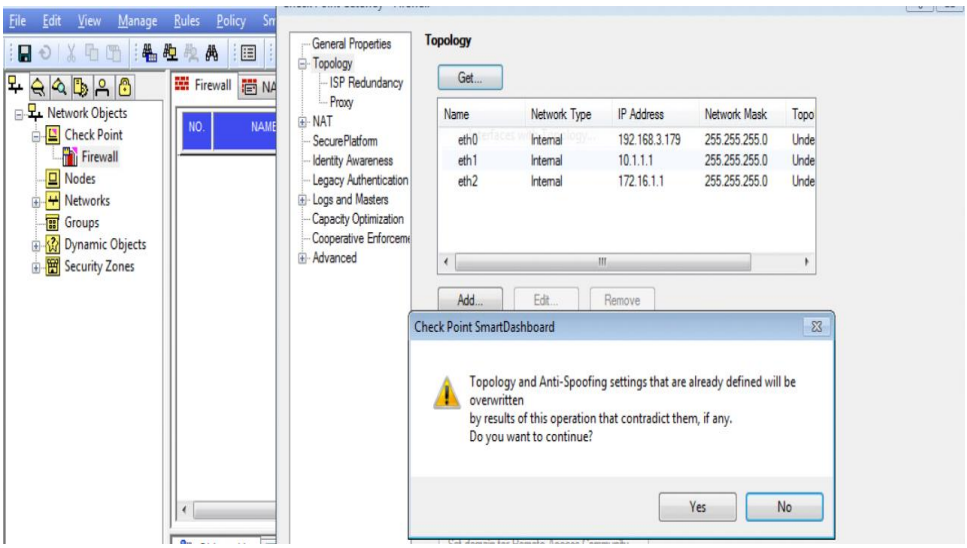


Xuất hiện giao diện quản trị:

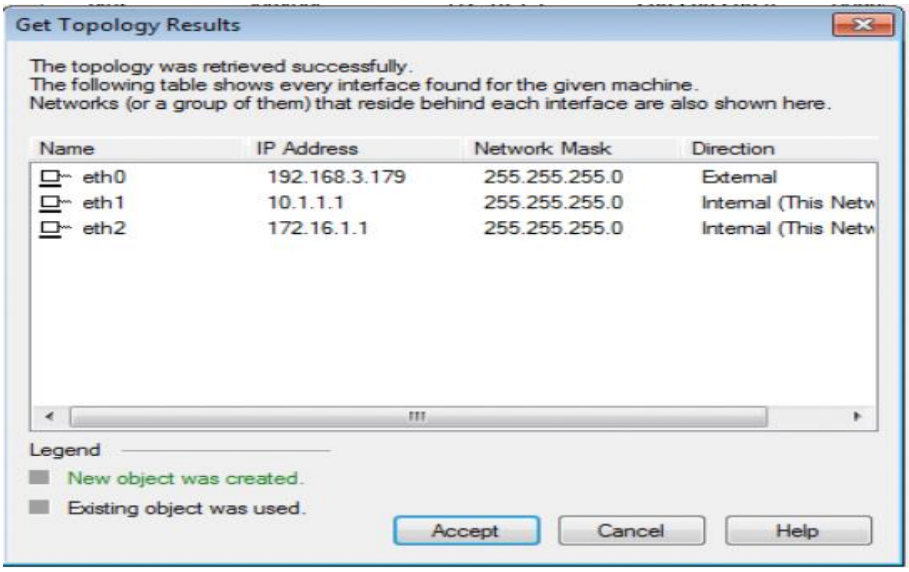


2.2.2. Cấu hình AntiSpoofing

Xác định các phân vùng mạng trên tường lửa: Click vào Check Point -> Firewall ->Topology -> Get -> Interface topology -> Yes.

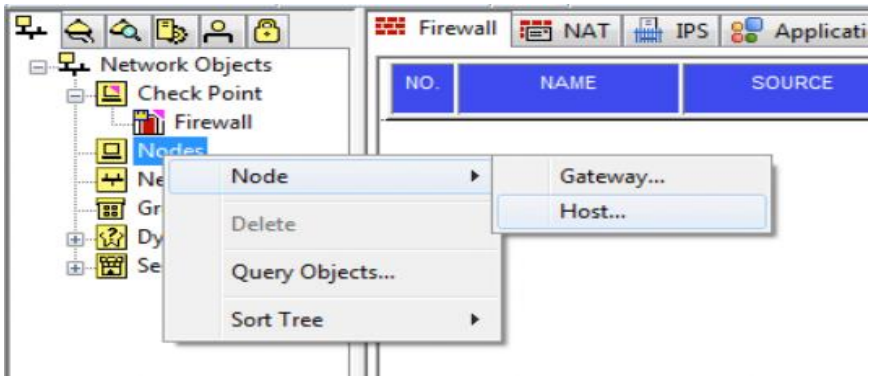


Click vào Accept để hoàn tất việc cấu hình AntiSpoofing



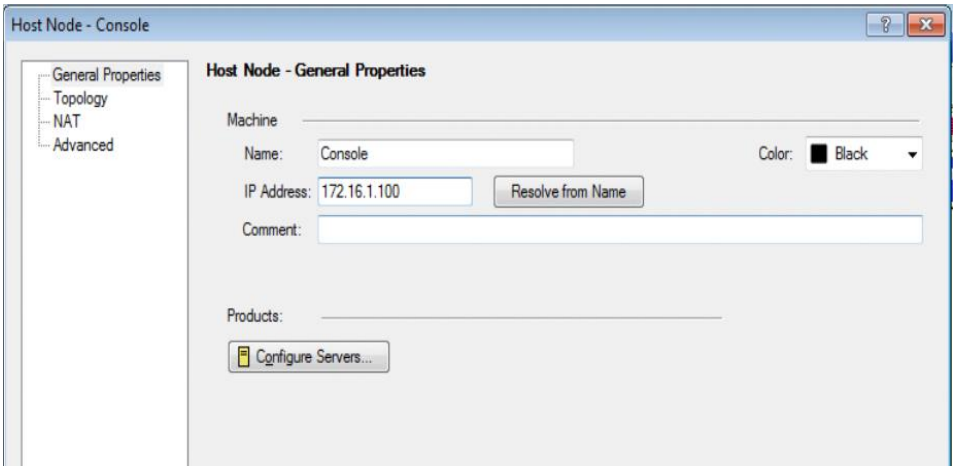
2.2.3. Tạo các Node mạng và dải mạng

Tiến hành tạo các node mạng: Click phải chuột vào Nodes chọn Node -> Host.

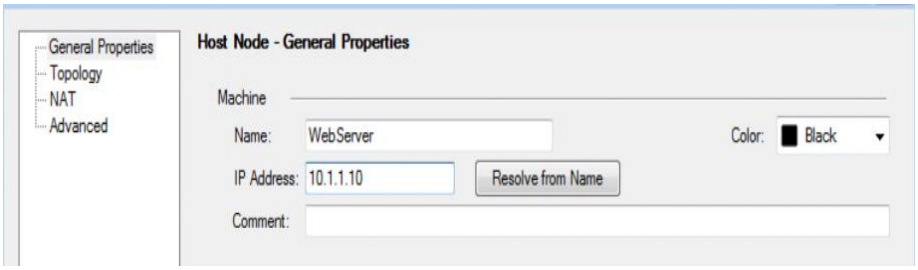


Điền các thông tin cụ thể về host như:

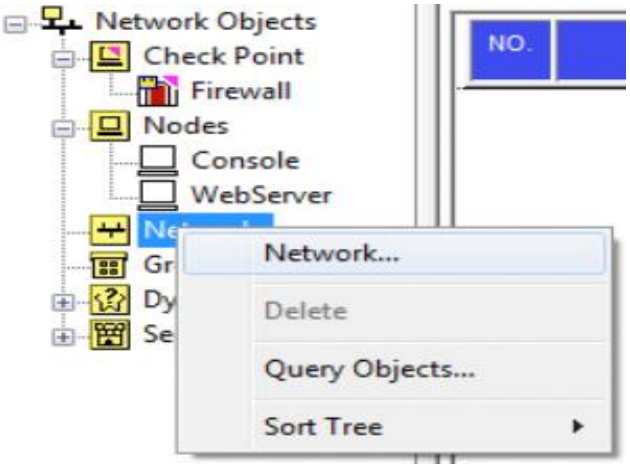
+ Name: Tên host (ví dụ: Console)
+ IP Address: Địa chỉ IP tương ứng với host (172.16.1.100)
+ Comment: Chú thích thêm về host
+ Ngoài ra có thể chọn các màu sắc khác nhau trong phần Color.



Thực hiện tương tự để tạo node cho máy chủ dịch vụ Web



Tiếp theo tạo các dải mạng tương ứng với các vùng mạng trong hệ thống: Click phải chuột vào Networks chọn Network

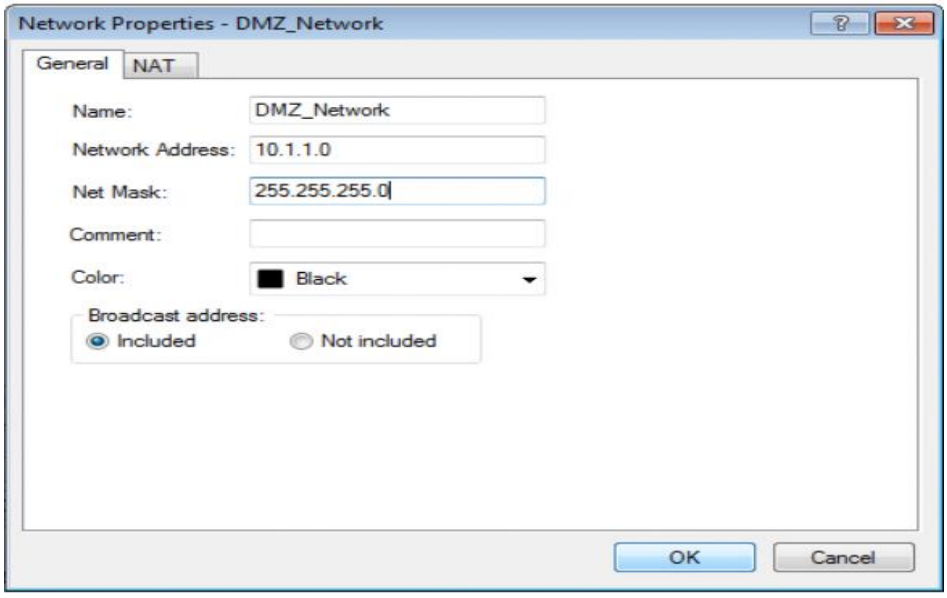


Định nghĩa dải mạng LAN:

+ Name: Tên dải mạng (LAN_Network)
+ Network Address: Dải địa chỉ của mạng (172.16.1.0)
+ Net Mask: Số lượng các máy tính có thể có trong mạng (255.255.255.0)

+ Comment: Chú thích thêm về host
+ Color: Lựa chọn màu sắc cho dải mạng

Thực hiện tương tự với dải mạng DMZ:



2.2.4. Thiết lập các luật cho tường lửa

Trên thanh tùy chỉnh chọn "Add rule at the buttom"

Luật đầu tiên: Chặn các truy cập trái phép vào tường lửa

Cấu hình các tham số cho luật:

+ Name: Stealth Rule
+ Source Any (Cho phép tất cả các nguồn truy cập)
+ Destination: Firewall
+ Service: any (Tất cả các dịch vụ)
+ Action: drop (Hủy bỏ tất cả các gói tin đi qua)
+ Track: Log (Có ghi lại nhật ký)
+ Install On: Firewall (Hoặc có thể để nguyên là Policy targets)
+ Time : Any

Luật thứ 2: Cho phép bên ngoài được truy cập vào WebServer với các dịch vụ http, https, dns và cho phép ping.

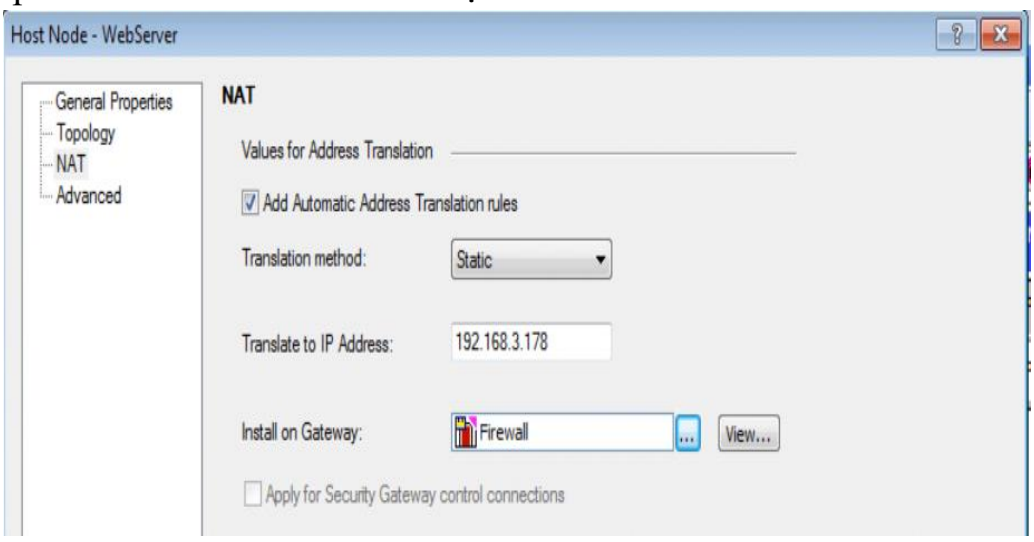
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Stealth Rule	* Any	Firewall	* Any Traffic	* Any	drop	Log	* Policy Targets	* Any
2	Web Rule	* Any	WebServer	* Any Traffic	http https dns echo-reply echo-request	accept	Log	* Policy Targets	* Any

Các tham số cho luật:

+ Name: Web Rule
+ Source: Any (Cho phép tất cả các nguồn truy cập)
+ Destination: WebServer (Chính là node ta đã tạo)
+ Service: http, https, dns, echo-reply và echo-request
+ Action: Accept (Cho phép đi qua tường lửa)
+ Track: Log (Có ghi lại nhật ký)
+ Install On: Firewall hoặc giữ nguyên Policy targets
+ Time: Any

Ngoài ra, để có thể quảng bá Webserver ra bên ngoài mà không muốn cho người sử dụng truy cập vào địa chỉ IP thực của WebServer thì sẽ tiến hành cấu hình NAT. Ở đây sẽ thực hiện cấu hình Static NAT.

Kích đúp vào host là Webserver -> chọn NAT:



+ Click vào "Add Automatic Address Translation rules"
+ Tại Translation method lựa chọn "Static"
+ Translate to IP Address nhập địa chỉ IP muốn NAT: 192.168.3.178
+ Install on Gateway: chọn tường lửa Firewall

Luật thứ 3: Cho phép từ SmartConsole được truy cập tới bất kỳ đâu để quản trị

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
2	Web Rule	* Any	WebServer	Any Traffic	https dns echo-reply echo-request	accept	Log	Policy Targets	Any
3	SmartConsole -> Any	Console	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any

Các tham số cho luật:

+ Name: SmartConsole -> Any
+ Source: Console
+ Destination: Any
+ Service: Any
+ Action: Accept
+ Track: Log

Luật thứ 4: Cấm người dùng trong vùng mạng LAN truy cập yahoo và chơi game Online

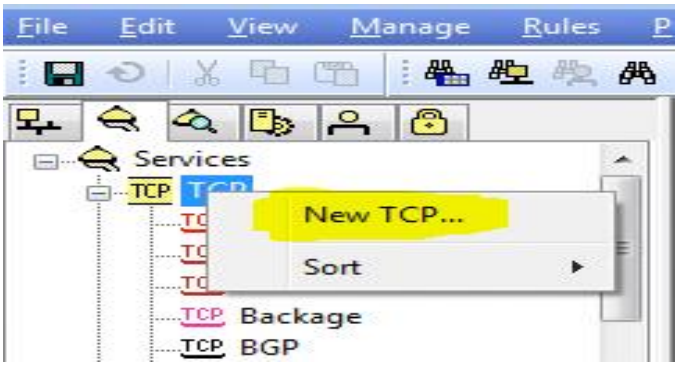
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
2	Web Rule	* Any	WebServer	Any Traffic	https dns echo-reply echo-request	accept	Log	Policy Targets	Any
3	SmartConsole -> Any	Console	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any
4	Deny LAN use Yahoo_Game	LAN_Network	* Any	Any Traffic	Yahoo_Messengr Yahoo_Messengr Yahoo_Messengr Cam_Game	drop	Log	Policy Targets	Any

Các tham số cho luật:

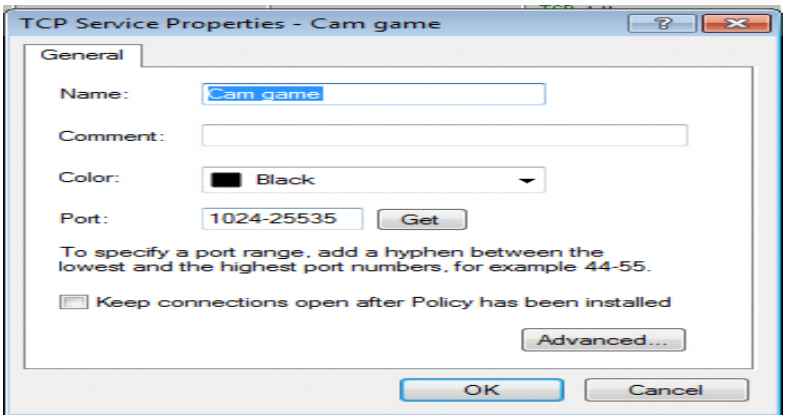
+ Name: Deny LAN use Yahoo_Game
+ Source: LAN_Network (dải mạng LAN ta định nghĩa ban đầu)
+ Destination: Any (Tất cả mọi điểm đến)
+ Service: Yahoo_Messenger_.... chọn tất cả các dịch vụ có liên quan đến Yahoo.

  Để thực hiện cấm chơi game online ta cần chặn các dịch vụ từ cổng 1024 trở lên theo giao thức TCP. Tuy nhiên trong tường lửa Check Point chưa có dịch vụ nào như thế được định nghĩa, do vậy ta cần định nghĩa 1 dịch vụ mới:

  - Chuyển sang tab Services -> click phải chuột vào TCP -> chọn New TCP



- Định nghĩa các thông tin liên quan:
  - Name: Đặt tên cho dịch vụ (Cam_game)
  - Comment: Chú thích thêm
  - Color: Lựa chọn màu sắc
  - Port: 1024-65535 (hoặc >1024)



+ Action: Drop (Hủy bỏ tất cả các gói tin đi qua)
+ Track: Log (Có ghi lại nhật ký)

Luật thứ 5: Chặn các truy cập trái phép từ vùng mạng LAN sang vùng mạng DMZ

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
2	Web Rule	* Any	WebServer	Any Traffic	https dns echo-reply echo-request	accept	Log	Policy Targets	Any
3	SmartConsole -> Any	Console	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any
4	Deny LAN use Yahoo _Game	LAN_Network	* Any	Any Traffic	Yahoo_Messeng Yahoo_Messeng Yahoo_Messeng Cam_Game	drop	Log	Policy Targets	Any
5	Deny LAN -> DMZ	LAN_Network	DMZ_Network	Any Traffic	* Any	drop	Log	Policy Targets	Any
6	Accept LAN -> Internet	LAN_Network	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any

Các tham số cho luật:

+ Name: Deny LAN -> DMZ
+ Source: LAN_Network
+ Destination: DMZ_Network

+ Service: Any
+ Action: Drop
+ Track: Log

Luật thứ 6: Cho phép vùng mạng LAN được truy cập ra ngoài Internet

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
2	Web Rule	* Any	WebServer	Any Traffic	https dns echo-reply echo-request	accept	Log	Policy Targets	Any
3	SmartConsole -> Any	Console	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any
4	Deny LAN use Yahoo ,Game	LAN_Network	* Any	Any Traffic	Yahoo_Messengo Yahoo_Messengo Yahoo_Messengo Cam_Game	drop	Log	Policy Targets	Any
5	Deny LAN -> DMZ	LAN_Network	DMZ_Network	Any Traffic	* Any	drop	Log	Policy Targets	Any
6	Accept LAN -> Internet	LAN_Network	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any

Các tham số cho luật:

+ Name: Accept LAN -> Internet
+ Source: LAN_Network
+ Destination: Any
+ Service: Any
+ Action: Accept
+ Track: Log

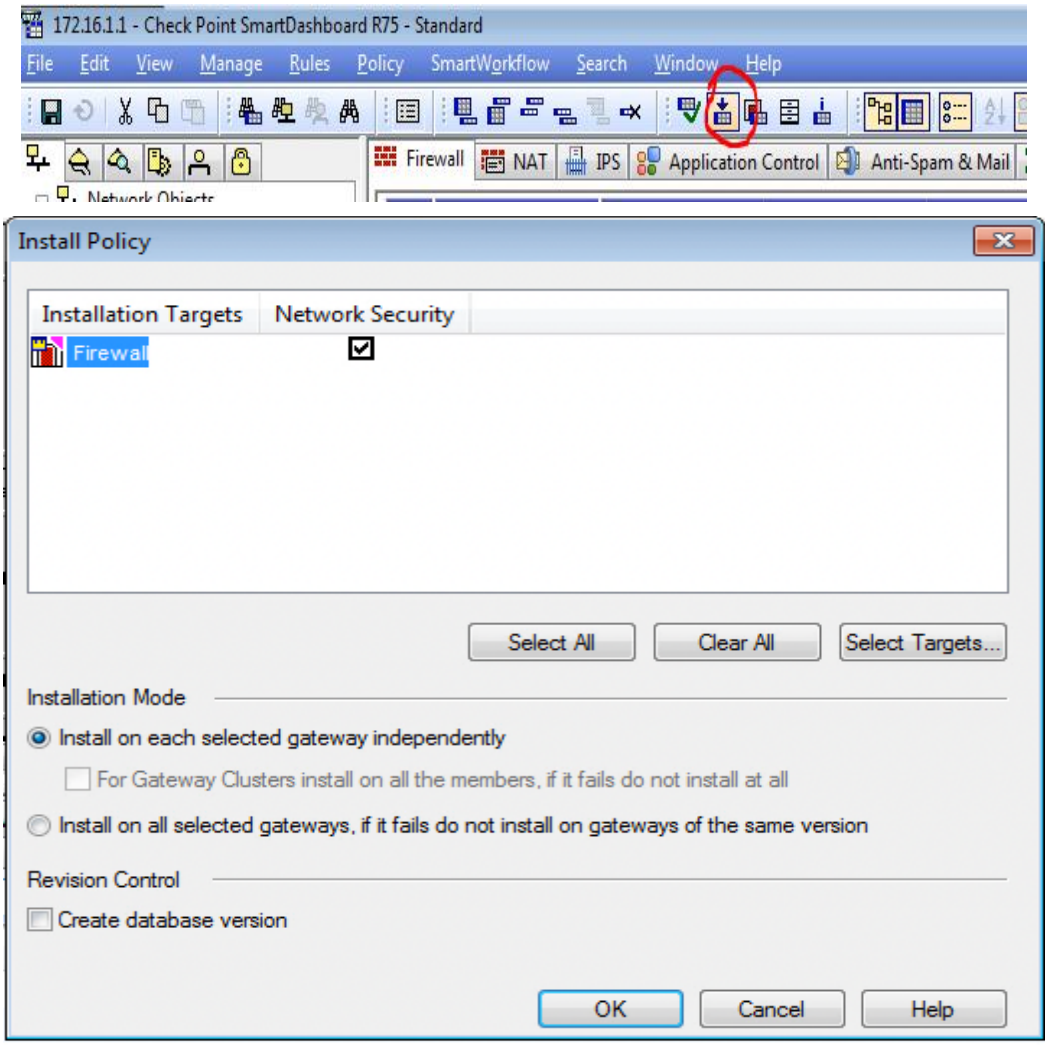
Luật thứ 7: Chặn tất cả các truy cập trái phép đi qua tường lửa

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
2	Web Rule	* Any	WebServer	Any Traffic	https dns echo-reply echo-request	accept	Log	Policy Targets	Any
3	SmartConsole -> Any	Console	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any
4	Deny LAN use Yahoo ,Game	LAN_Network	* Any	Any Traffic	Yahoo_Messengo Yahoo_Messengo Yahoo_Messengo Cam_Game	drop	Log	Policy Targets	Any
5	Deny LAN -> DMZ	LAN_Network	DMZ_Network	Any Traffic	* Any	drop	Log	Policy Targets	Any
6	Accept LAN -> Internet	LAN_Network	* Any	Any Traffic	* Any	accept	Log	Policy Targets	Any
7	Cleanup	* Any	* Any	Any Traffic	* Any	drop	Log	Policy Targets	Any

Các tham số cho luật:

+ Name: Clearup
+ Source: Any
+ Destination: Any
+ Service: Any
+ Action: Drop
+ Track: Log

Sau khi xây dựng xong các chính sách, trên thanh menu click vào Install policies -> OK



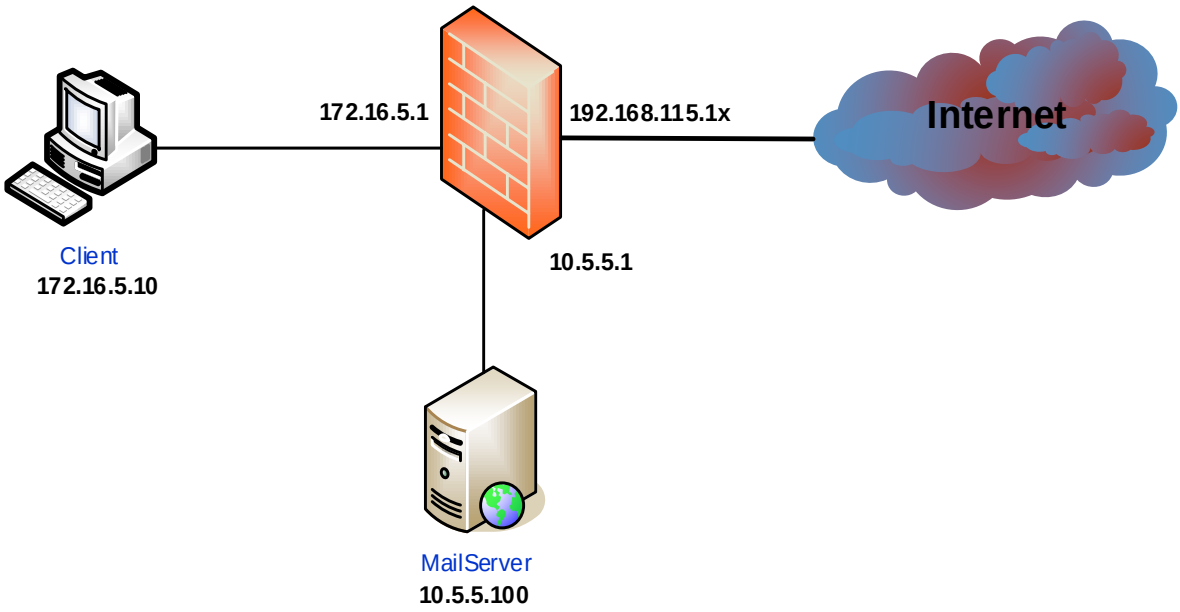
Chọn OK và đợi các tập luật được firewall áp dụng

Tất cả các tập luật trong check point sẽ được thực hiện từ trên xuống dưới. Tập luật nào nằm vị trí đầu tiên sẽ được thực hiện và có hiệu lực cao hơn các tập luật nằm ở bên dưới

PHẦN 3. SINH VIÊN TỰ THỰC HÀNH

3.1. Bài thực hành 1

Xây dựng mô hình mạng theo sơ đồ sau:



Sinh viên thực hiện cài đặt các máy như sau:

❖ **Máy ảo 1 (Firewall CheckPoint):**

- Cài đặt Firewall CheckPoint theo mô hình StandAlone trên nền tảng SecurePlatform
- Sử dụng 03 giao diện mạng như sau:
  + Địa chỉ IP: 192.168.115.x. Bridge
  + Địa chỉ IP: 172.16.5.1 (là địa chỉ IP của Firewall). VMNet3
  + Địa chỉ IP: 10.5.5.1. VMNet2

❖ **Máy ảo 2 (MailServer):**

- Cài đặt hệ điều hành Windows Server 2003 SP2
- Cài đặt dịch vụ Mdaemon Mail Server
- Tạo 2 tài khoản email
- Địa chỉ IP: 10.5.5.100

❖ **Máy ảo 3 (Client):**

- Cài đặt hệ điều hành Windows XP hoặc Windows 7
- Cài đặt SmartConsole
- Địa chỉ IP: 172.16.5.10

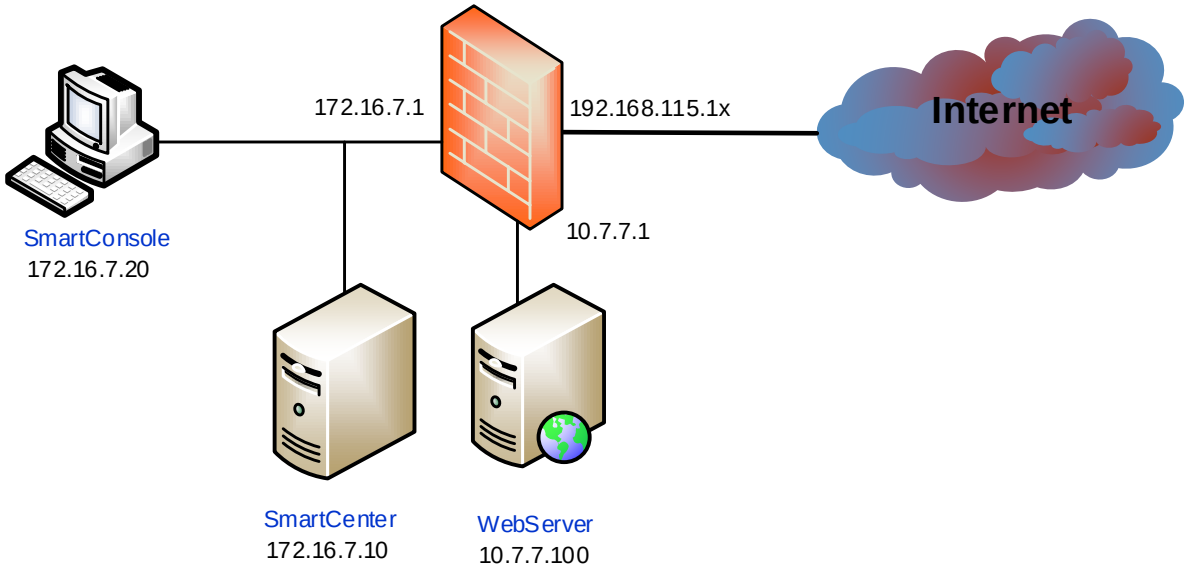
Yêu cầu:

- Cấu hình Anti-Spoofing cho Firewall.
- Thiết đặt các luật trên Firewall sao cho:
  + Chặn tất cả các truy cập trái phép vào Firewall.

+ Sử dụng NAT để quảng bá MailServer ra ngoài, sao cho người sử dụng khi cấu hình gửi nhận email sử dụng dịch vụ SMTP và POP3 sẽ phải sử dụng IP đã quảng bá.
+ Cho phép các máy trong mạng LAN được phép truy cập ra Internet nhưng cấm chơi game online (port>1024) trong khoảng thời gian từ 08h00 – 17h00, ngoài khoảng thời gian này các máy trong mạng LAN được toàn quyền sử dụng dịch vụ Internet.
+ Chỉ có máy Client mới được phép truy cập vào vùng DMZ (10.5.5.0/24) để quản trị, còn lại các máy khác dù có trong vùng mạng LAN cũng không được phép truy cập vào vùng mạng trên ngoài các dịch vụ được phép.
+ Tất các các truy cập khác đều bị cấm.

3.2. Bài thực hành 2

Xây dựng mô hình mạng theo sơ đồ sau:



Sinh viên thực hiện cài đặt các máy như sau:

❖ **Máy ảo 1 (Firewall CheckPoint):**
- Cài đặt Firewall CheckPoint theo mô hình Distributed *(phần cài đặt theo mô hình Distributed sinh viên tự tham khảo trên mạng)* trên nền tảng SecurePlatform
- Sử dụng 03 giao diện mạng như sau:
  + Địa chỉ IP: 192.168.115.x. Bridge
  + Địa chỉ IP: 172.16.7.1. (là địa chỉ IP của Firewall). VMNet 2
  + Địa chỉ IP: 10.7.7.1. VMNet 3

❖ **Máy ảo 2 (SmartConsole):**
- Cài đặt hệ điều hành Windows XP hoặc Windows 7
- Cài đặt SmartConsole
- Cấu hình mở dịch vụ Remote Desktop.
- Địa chỉ IP: 172.16.7.20. VMNet 2

❖ **Máy ảo 2 (SmartCenter):**
- Cài đặt hệ điều hành Windows Server 2003 SP2
- Cài đặt SmartCenter
- Địa chỉ IP: 172.16.7.10. VMNet 2

❖ **Máy ảo 3 (WebServer):**
- Cài đặt hệ điều hành Windows Server 2003 SP2
- Cài đặt dịch vụ WebServer
- Tạo 1 Website đơn giản để có thể truy cập tới WebServer
- Địa chỉ IP: 10.7.7.100. VMNet 3

Yêu cầu:
- Cấu hình Anti-Spoofing cho Firewall.
- Thiết đặt các luật trên Firewall sao cho:
  + Chặn tất cả các truy cập trái phép vào Firewall.
  + Sử dụng NAT quảng bá WebServer ra bên ngoài, chỉ cho phép người sử dụng truy cập vào WebServer qua giao thức HTTP và HTTPS, cho phép ping.
  + Cho phép bên ngoài thực hiện dịch vụ Remote Desktop vào SmartConsole để quản trị.
  + Tất các các truy cập khác đều bị cấm.