

## BÁO CÁO BÀI LAB SỐ 03

### 1. Port Security

**1.1:** Cấu hình port security. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch.

**1.2:** Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

Câu lệnh:

Switch(config)#int f0/1

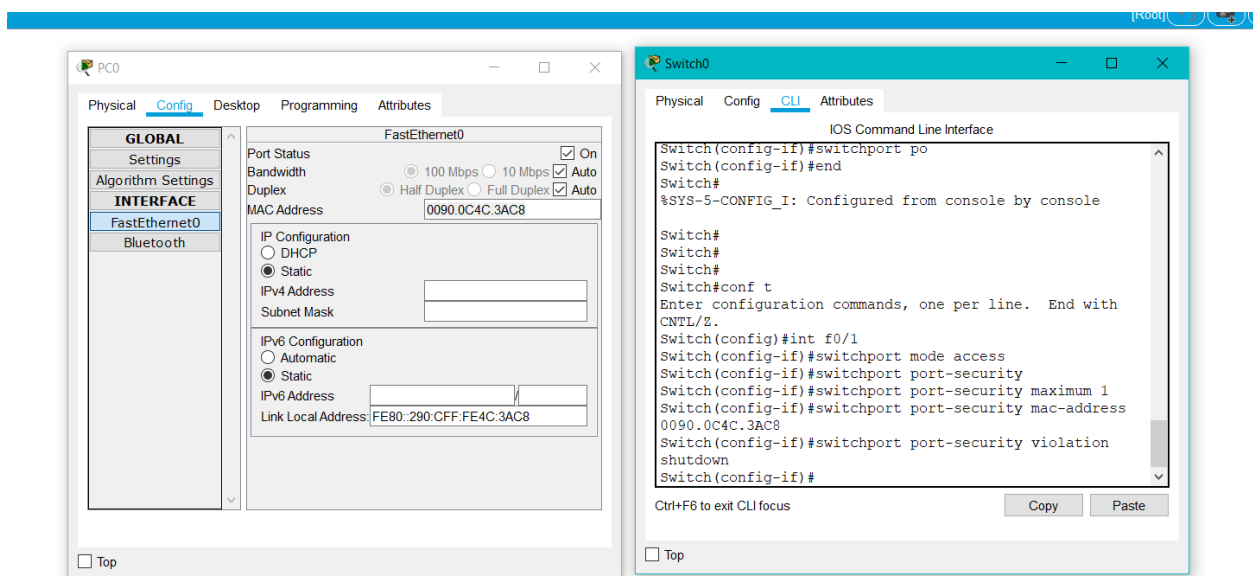
Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security maximum 1

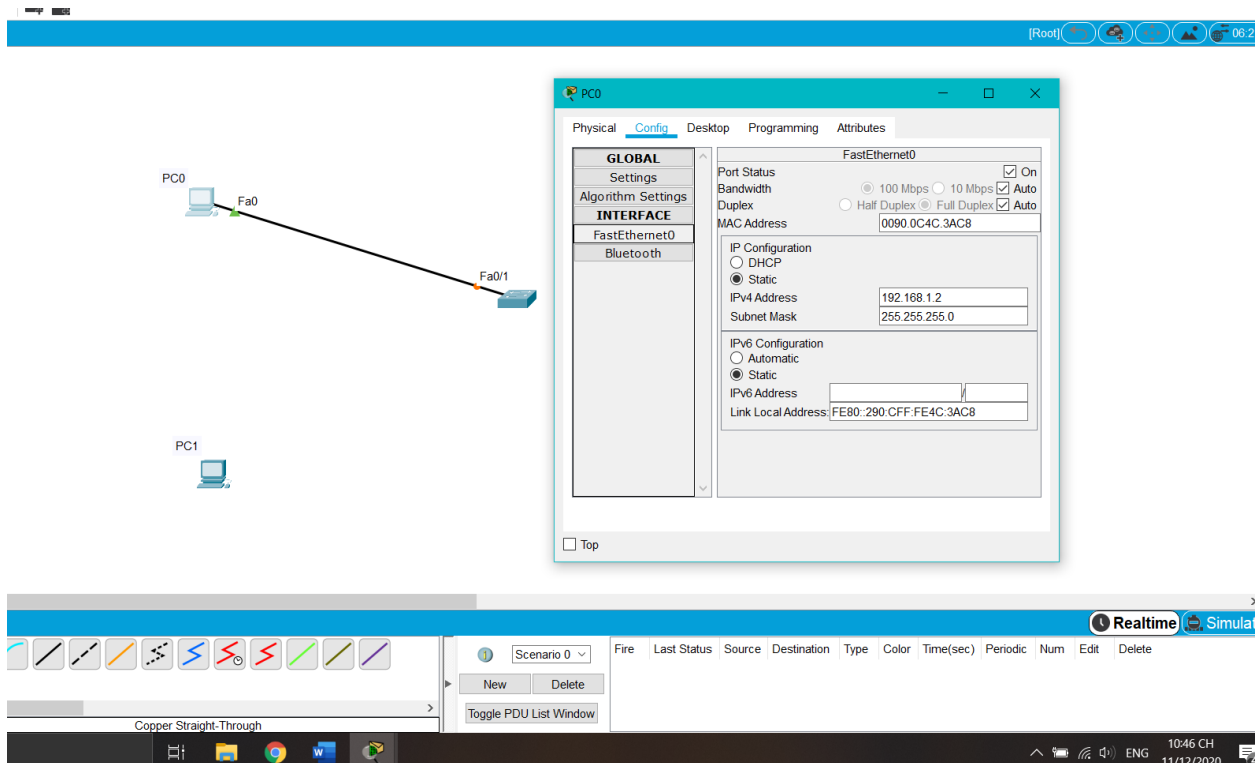
Switch(config-if)#switchport port-security mac-address 0090.0C4C.3AC8

Switch(config-if)#switchport port-security violation shutdown

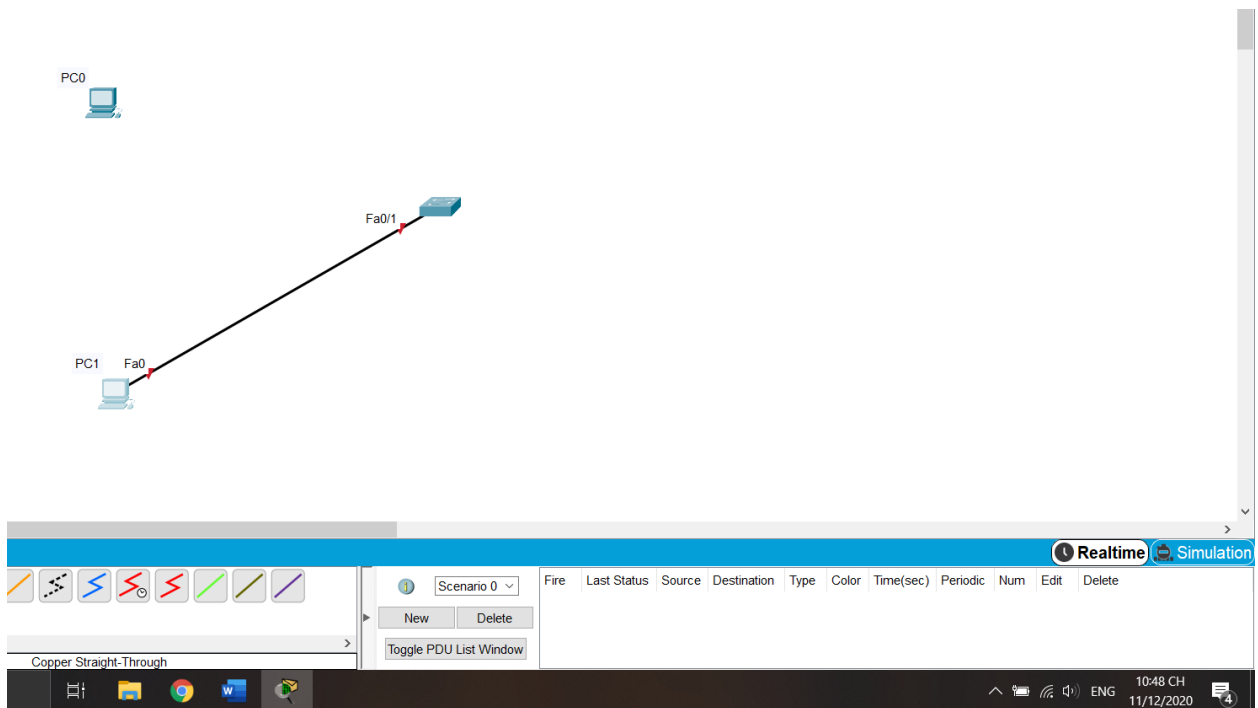


Kiểm tra cài đặt

- Nối dây PC0 với cổng f0/1 (thành công)

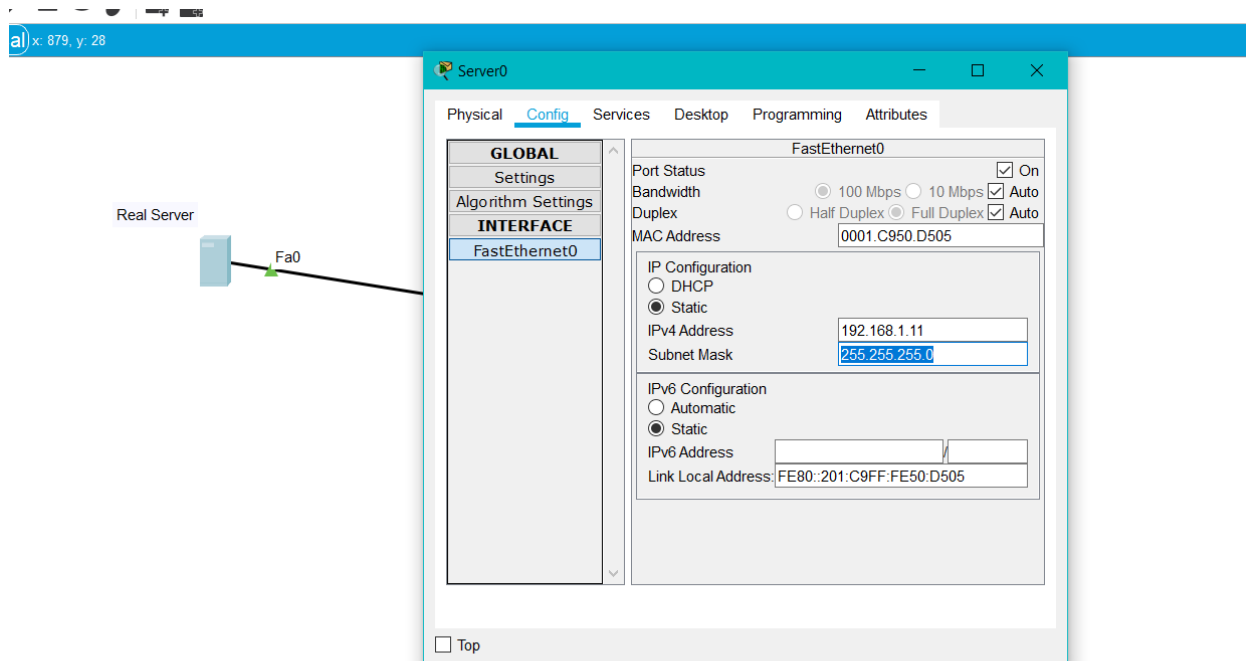


- Nối PC1 với cổng f0/1 (thất bại)

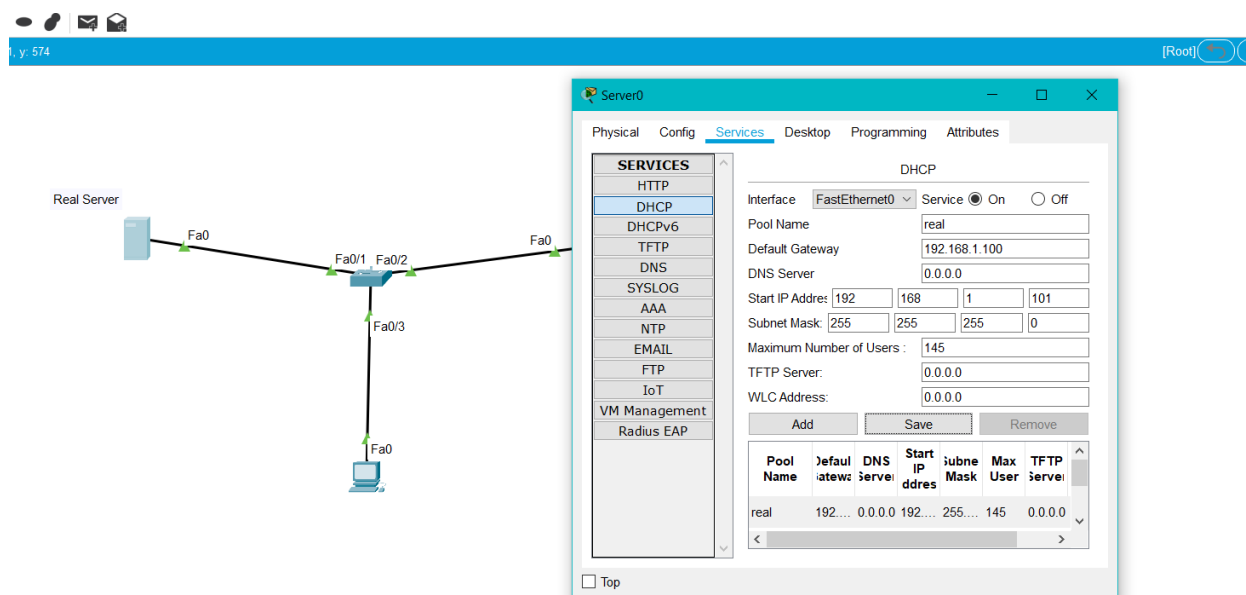


## 2. DHCP snooping

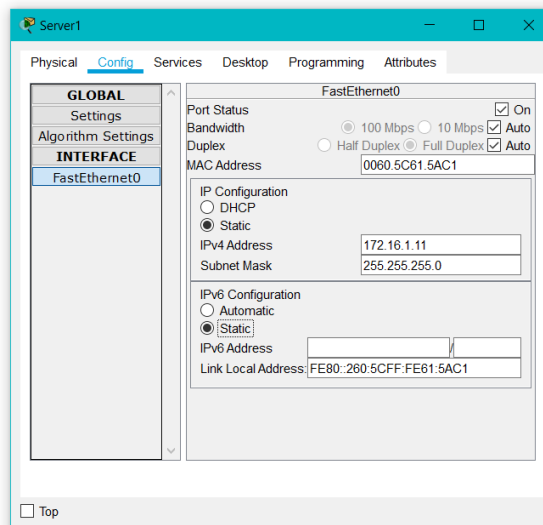
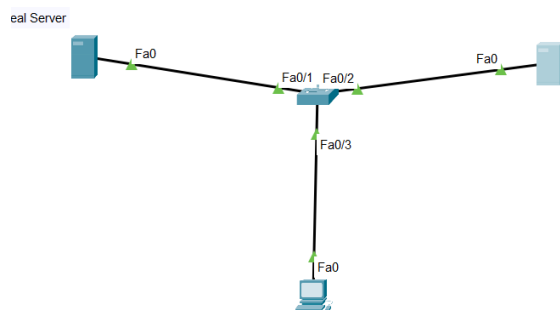
- Cấu hình cho Real Server



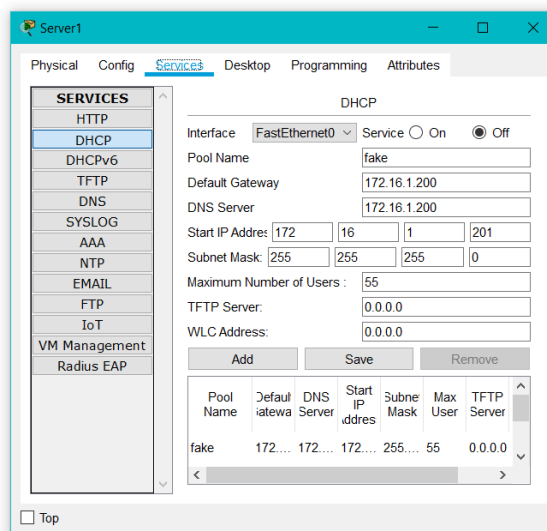
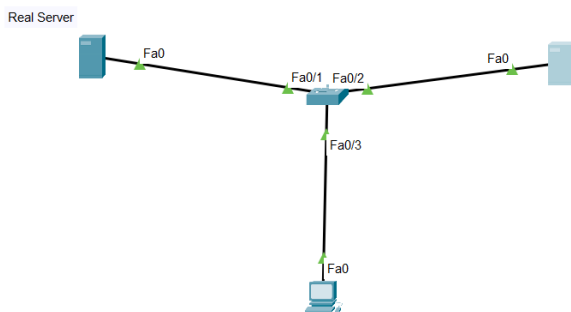
- Cấu hình dịch vụ DHCP cho Real Server



- Cấu hình cho Fake Server



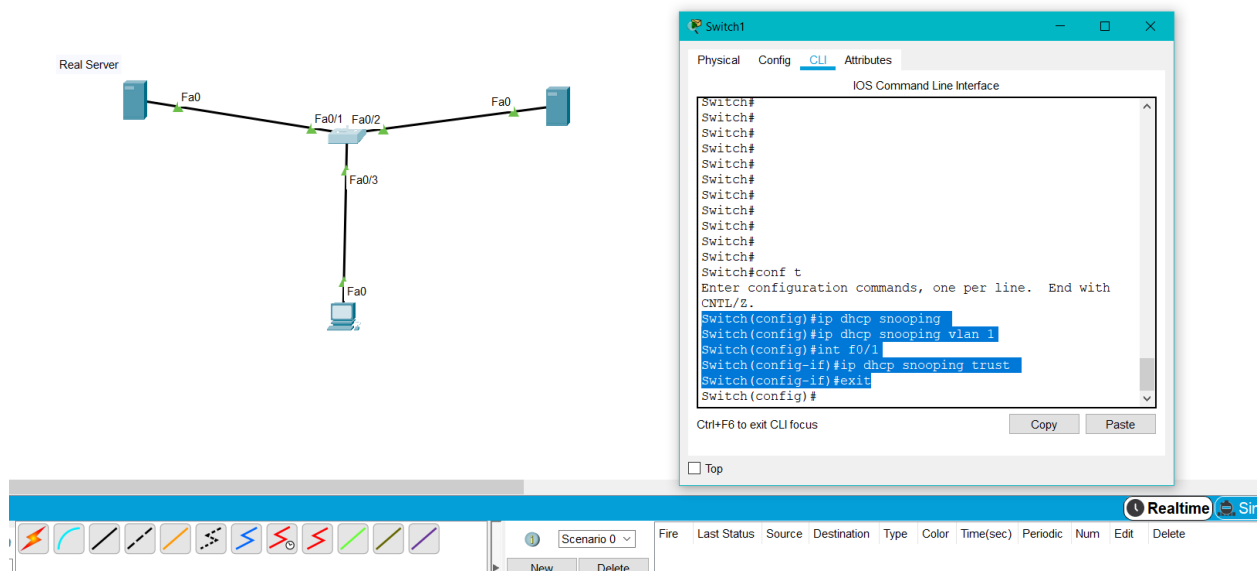
- Cấu hình dịch vụ DHCP cho Fake Server



- Cấu hình cho Switch chỉ nhận DHCP từ Real Server (nối cổng f0/1)

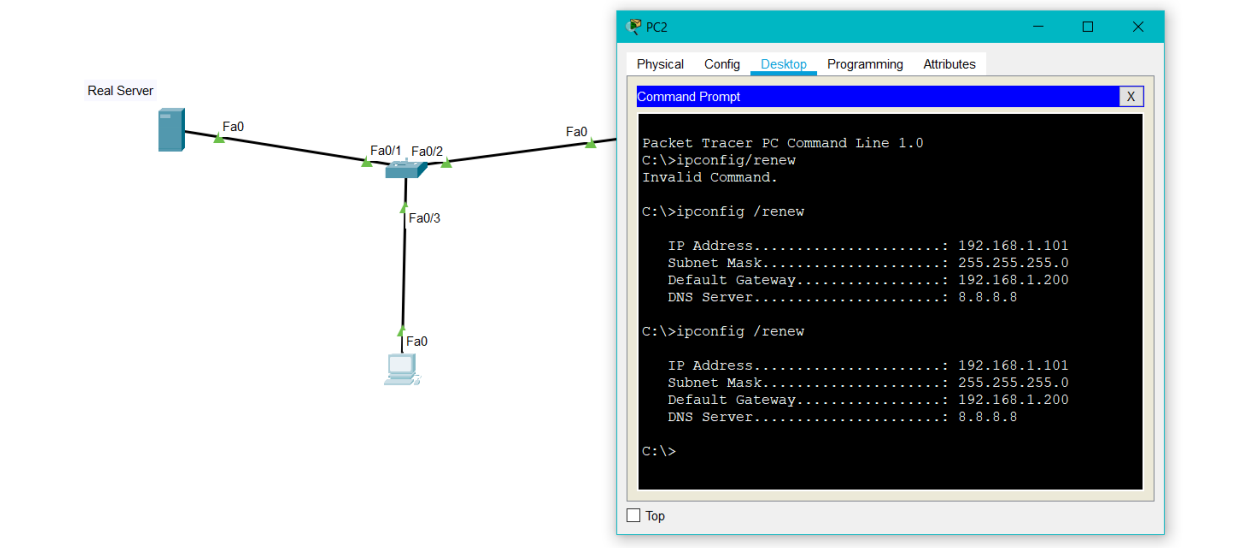
Câu lệnh:

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int f0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
```



- Kiểm tra cài đặt

Xin địa chỉ IP => chỉ nhận IP được cấp từ Real Server



### 3. Firewall

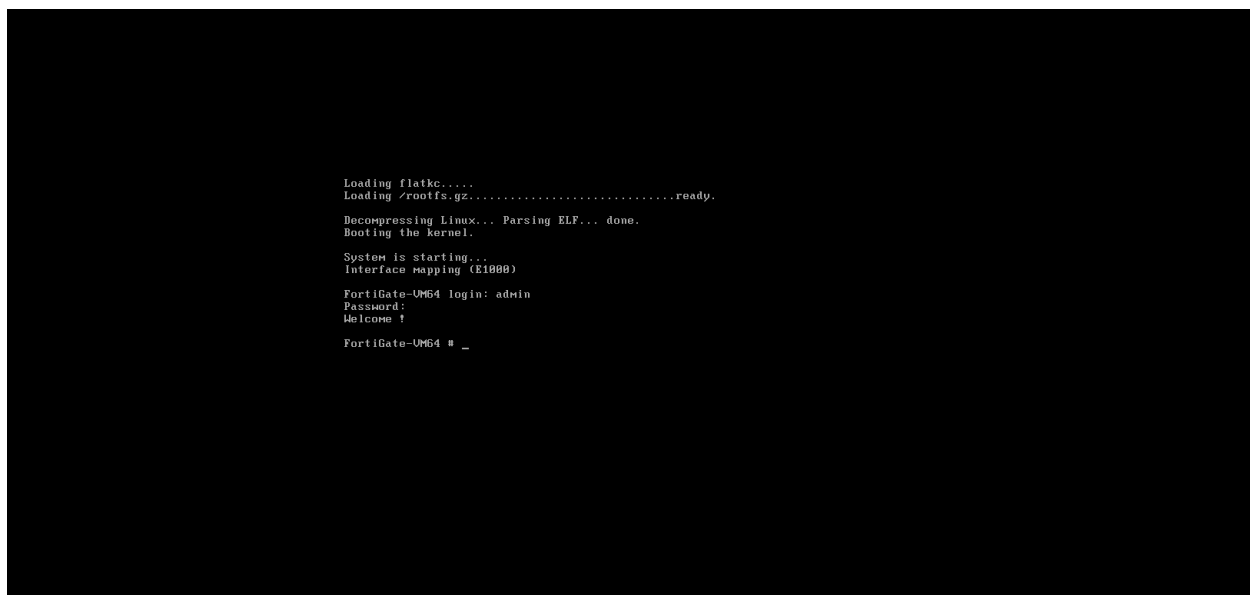
#### 3.1 Cài đặt Firewall Fortigate:

- 1) Tải bộ cài đặt máy chủ Firewall Fortigate trên VMWare tại <https://www.fshare.vn/file/H5XYU2FPYIE6?token=1607594438>

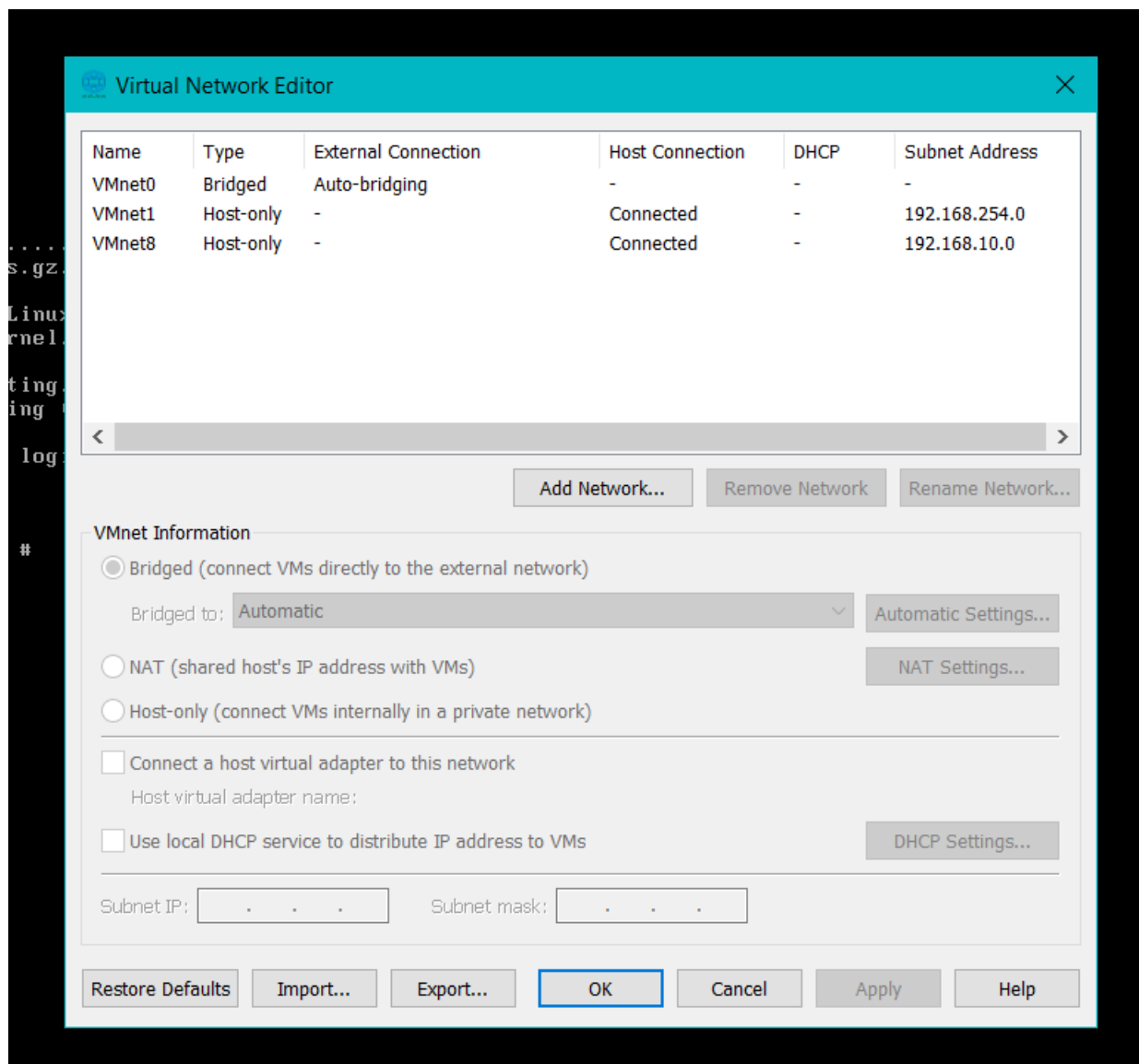
- 2) Sau đó giải nén ra và import vào VMWare
- 3) Sau khi import thành công



- 4) Login vào với tài khoản là admin (không có password )



- 5) Vào bảng các card mạng của VMWare và ghi nhớ các địa chỉ IP này



6) Gõ các câu lệnh như sau để cấu hình cho port1

```

Welcome :

FortiGate-UM64 # config system interface

FortiGate-UM64 (interface) # set po
command parse error before 'set'

FortiGate-UM64 (interface) # edit port1

FortiGate-UM64 (port1) # set ip 192.168.10.1 255.255.255.0

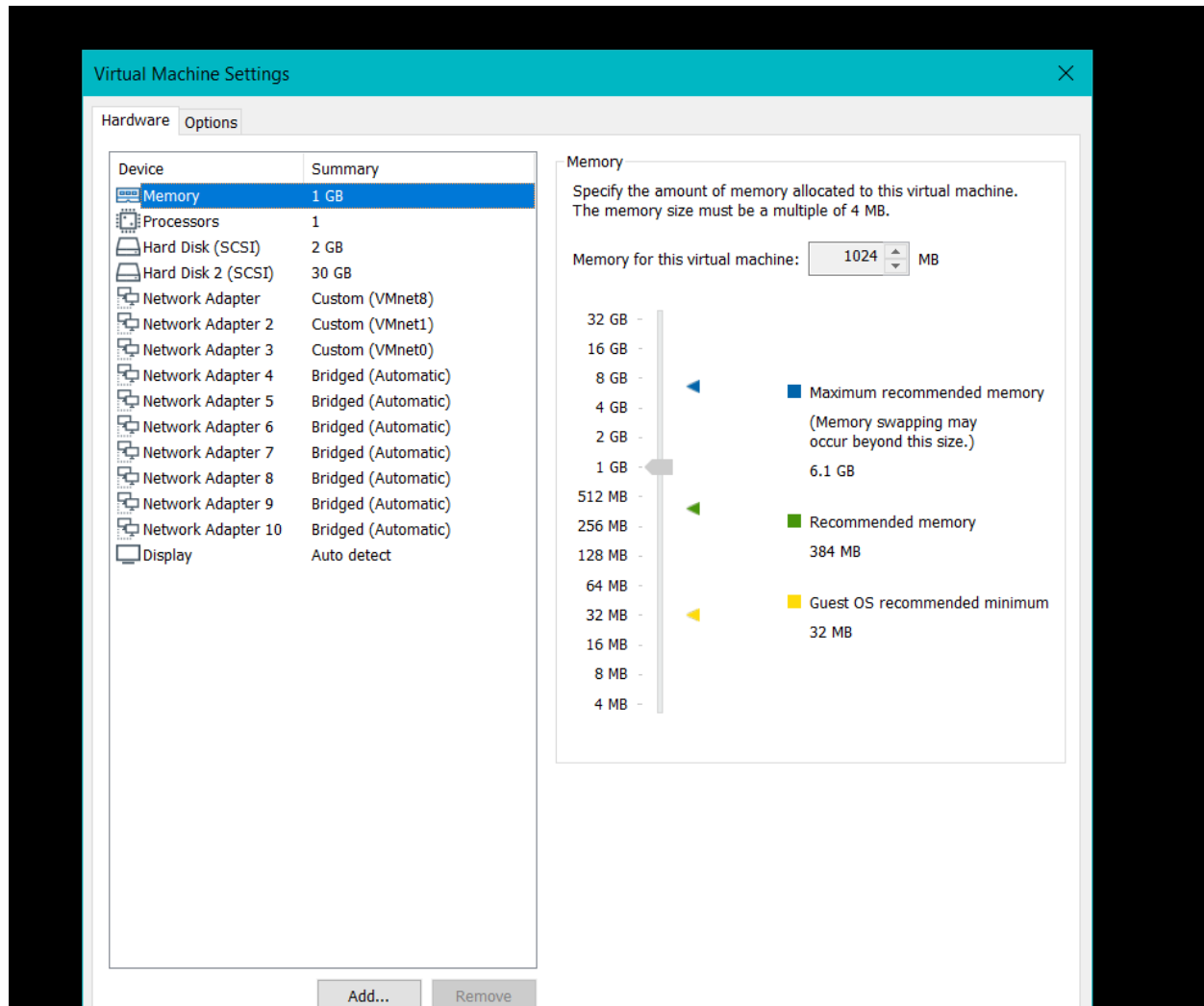
FortiGate-UM64 (port1) # set allowaccess https http ssh telnet ping

FortiGate-UM64 (port1) # end

```

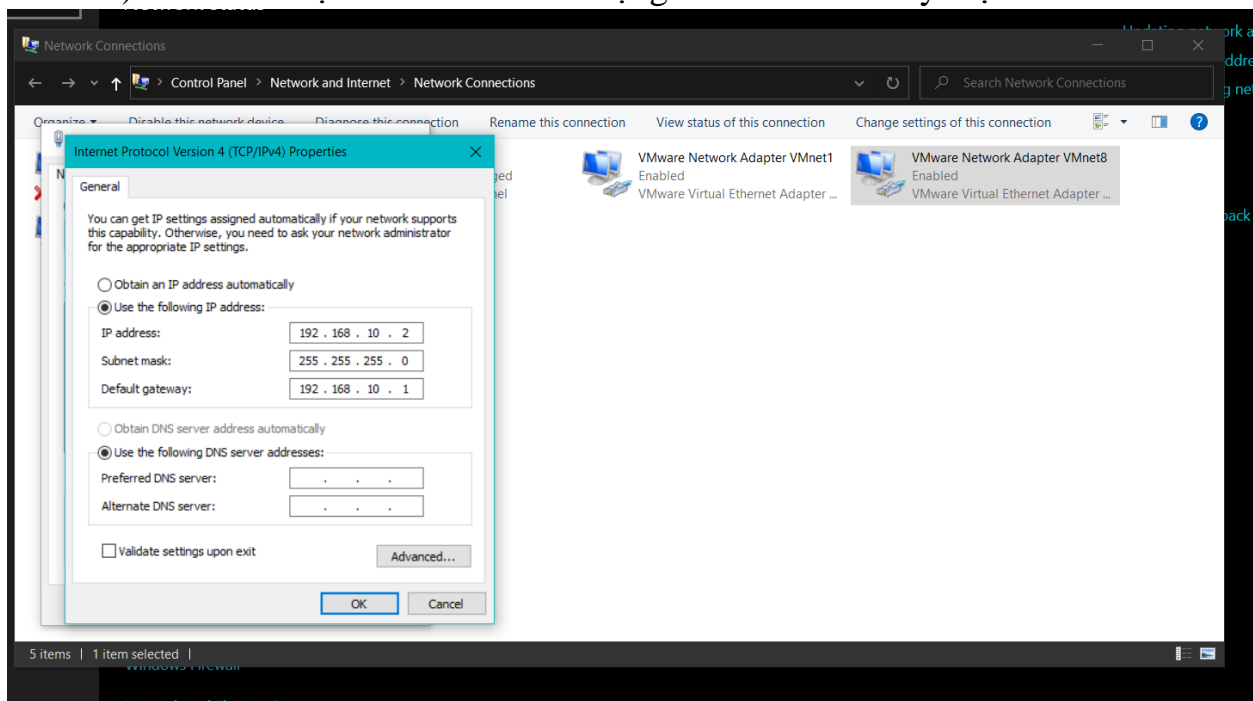
- Câu lệnh set allowaccess https http ssh telnet ping là để ta có quyền truy cập thông qua giao diện web từ xa

## 7) Điều chỉnh card mạng của máy chủ Firewall để kết nối với Vmnet8

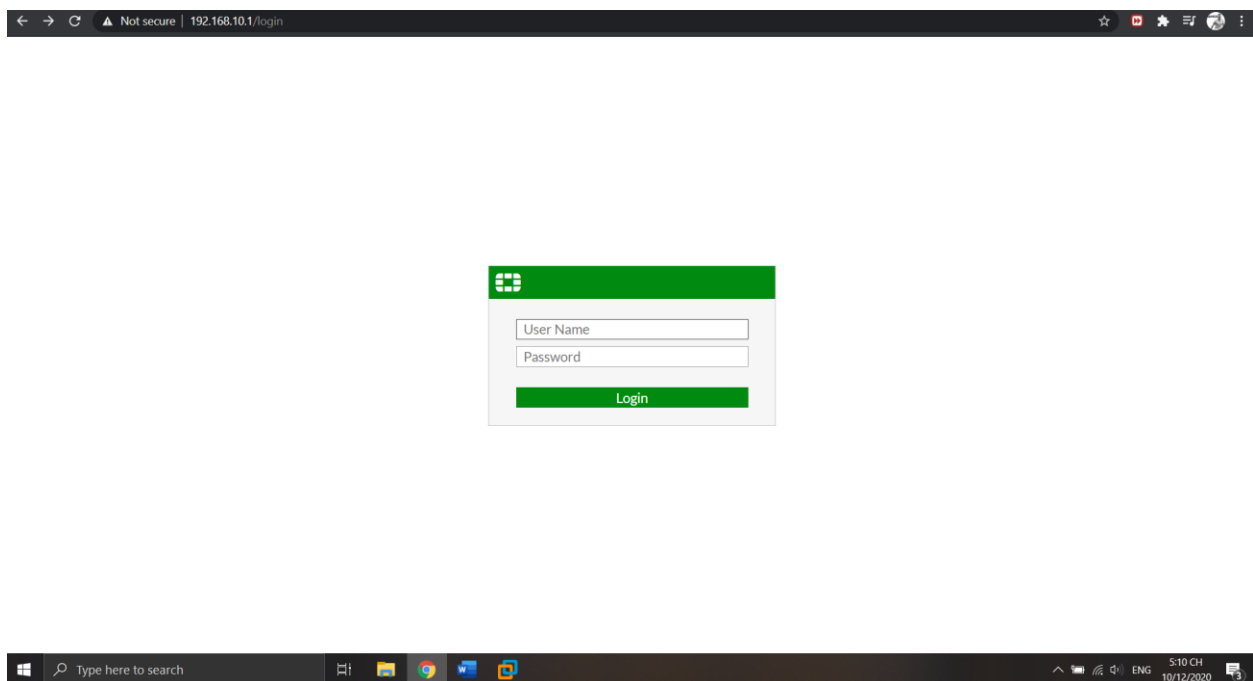




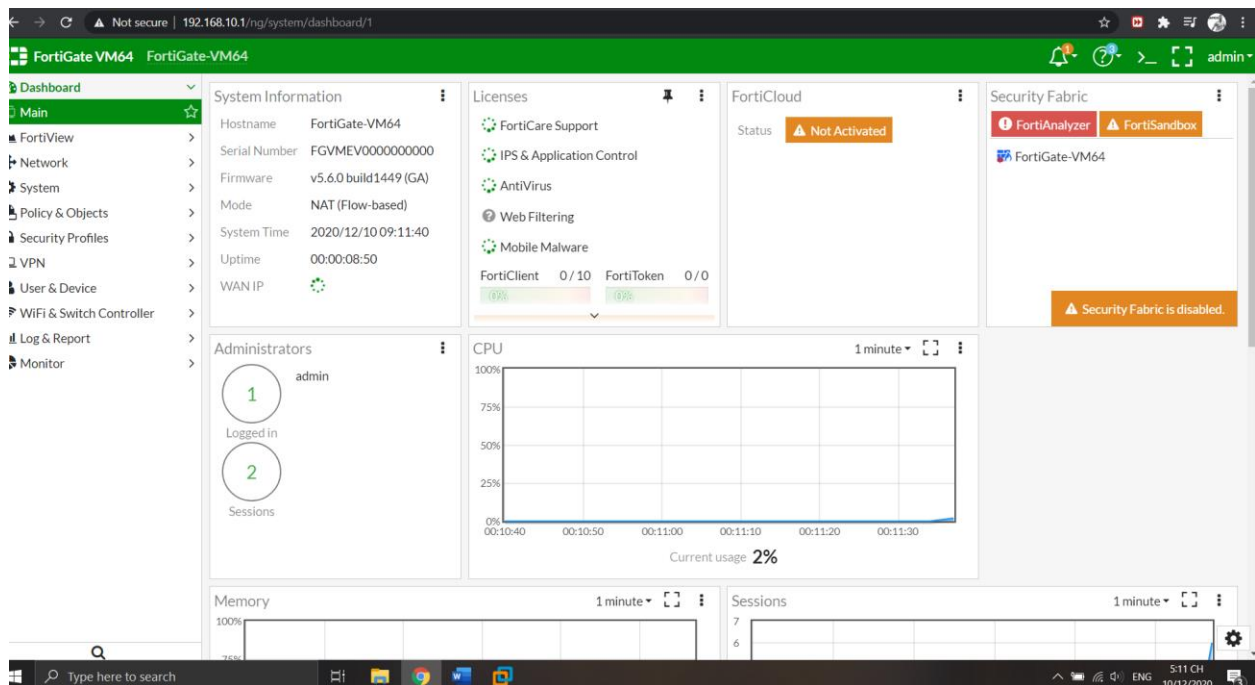
## 8) Cấu hình địa chỉ IP của card mạng Vmnet8 trên máy thật



## 9) Vào web browser nhập địa chỉ đã cấu hình cho máy chủ Firewall

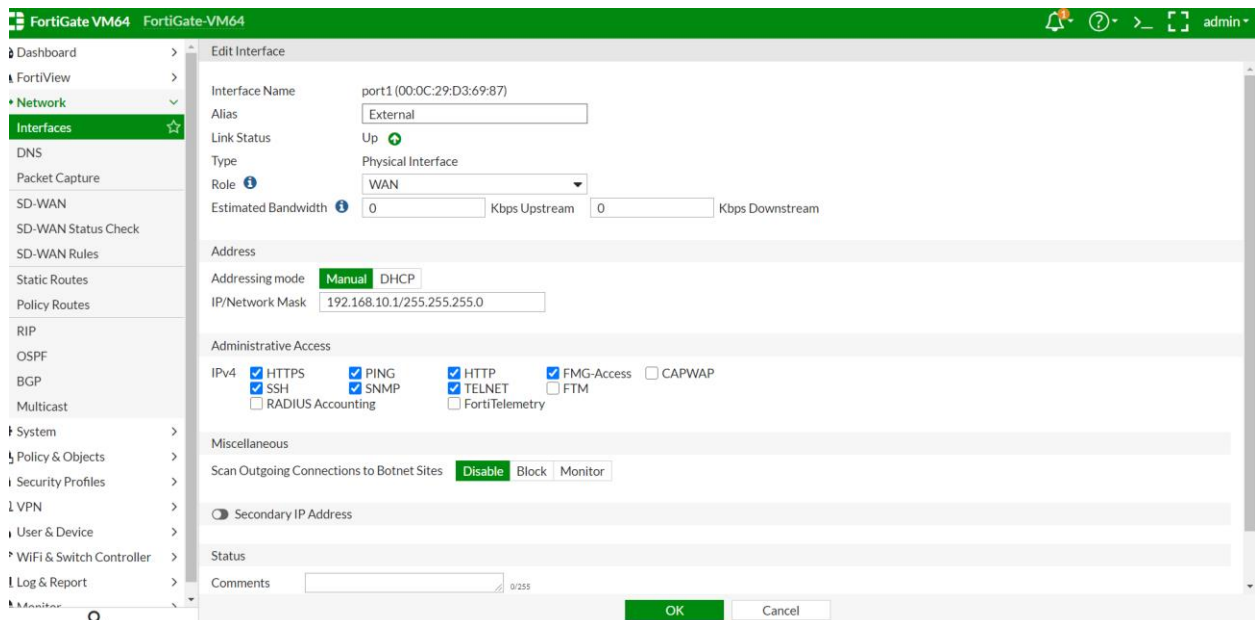


10) Nhập tài khoản là admin (không có password) ta vào giao diện như dưới đây



### 3.2 Thiết lập các rule:

Setting cấu hình của port1 ( ra ngoài Internet ) như sau:



Setting cấu hình cho port2 ( nối với mạng LAN ) như sau:

FortiGate VM64 FortiGate-VM64

Dashboard FortiView Network Interfaces DNS Packet Capture SD-WAN SD-WAN Status Check SD-WAN Rules Static Routes Policy Routes RIP OSPF BGP Multicast System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report Monitor

### Edit Interface

Interface Name: port2 (00:0C:29:D3:69:91)  
 Alias: LAN  
 Link Status: Up  
 Type: Physical Interface  
 Role: LAN

Address  
 Addressing mode: Manual DHCP One-Arm Sniffer Dedicated to FortiSwitch  
 IP/Network Mask: 172.16.1.1/255.255.255.0

Administrative Access  
 IPv4: ☒ HTTPS ☒ PING ☒ FMG-Access ☒ CAPWAP ☒ SSH  
☒ SNMP ☐ FTM ☐ RADIUS Accounting ☐ FortiTelemetry

☐ DHCP Server

Networked Devices

Device Detection: ☐

Admission Control

Security Mode: None

OK Cancel

a) Cho phép các PC trong mạng nội bộ ra ngoài Internet

Vào Network => Static Routes

FortiGate VM64 Firewall

Dashboard FortiView Network Interfaces DNS Packet Capture SD-WAN SD-WAN Status Check SD-WAN Rules Static Routes Policy Routes RIP OSPF BGP Multicast System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report Monitor


### New Static Route

Destination: Subnet Named Address Internet Service  
 0.0.0.0/0.0.0.0  
 Device:   
 Gateway: 0.0.0.0  
 Administrative Distance: 10  
 Comments:   
 Status: ☒ Enabled ☐ Disabled


Advanced Options

OK Cancel


Edit Static Route


Destination  **Subnet** | Named Address | Internet Service



0.0.0.0/0.0.0.0


Device  External (port1)

Gateway 192.168.1.1

Administrative Distance  10

Comments  0/255

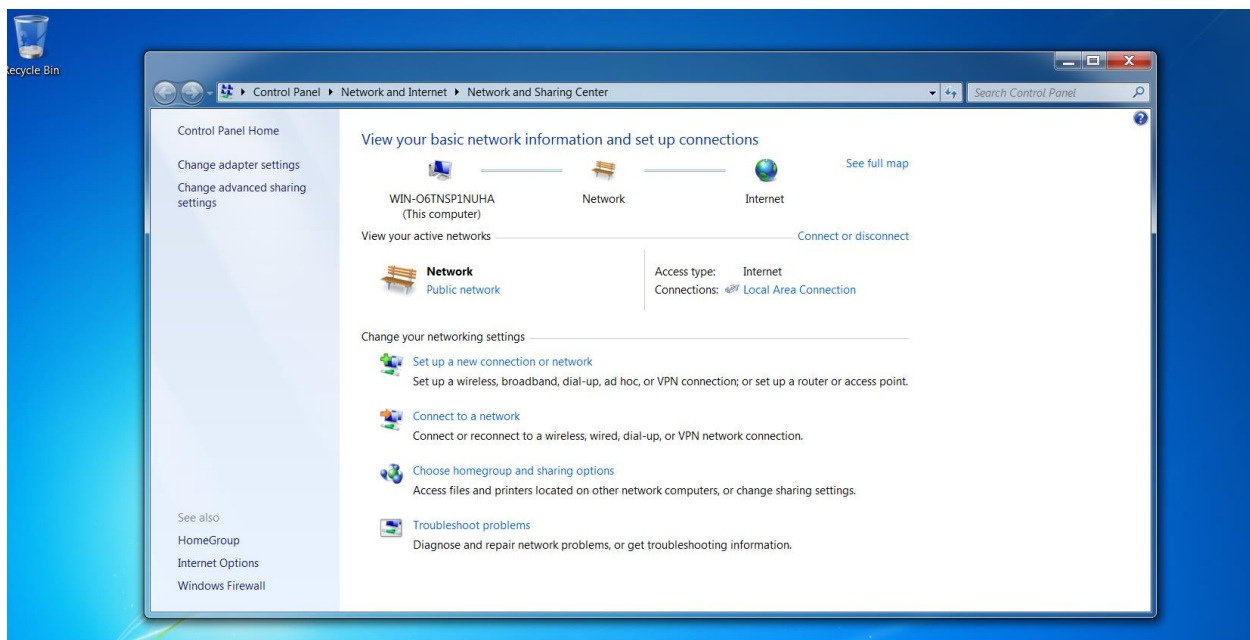
Status  Enabled  Disabled

 Advanced Options

OK Cancel

- 0.0.0.0/0.0.0.0 tức là cho toàn bộ các dải mạng LAN ra ngoài Internet. Cũng có thể cho cụ thể một mạng nào đó
- Device: cổng ra Internet ( tức là cổng WAN )
- Gateway: địa chỉ ra Internet

Kiểm tra trên Client => NAT thành công ra ngoài Internet



Vào mục Policy & Objects => IPv4 Policy => Create New Policy

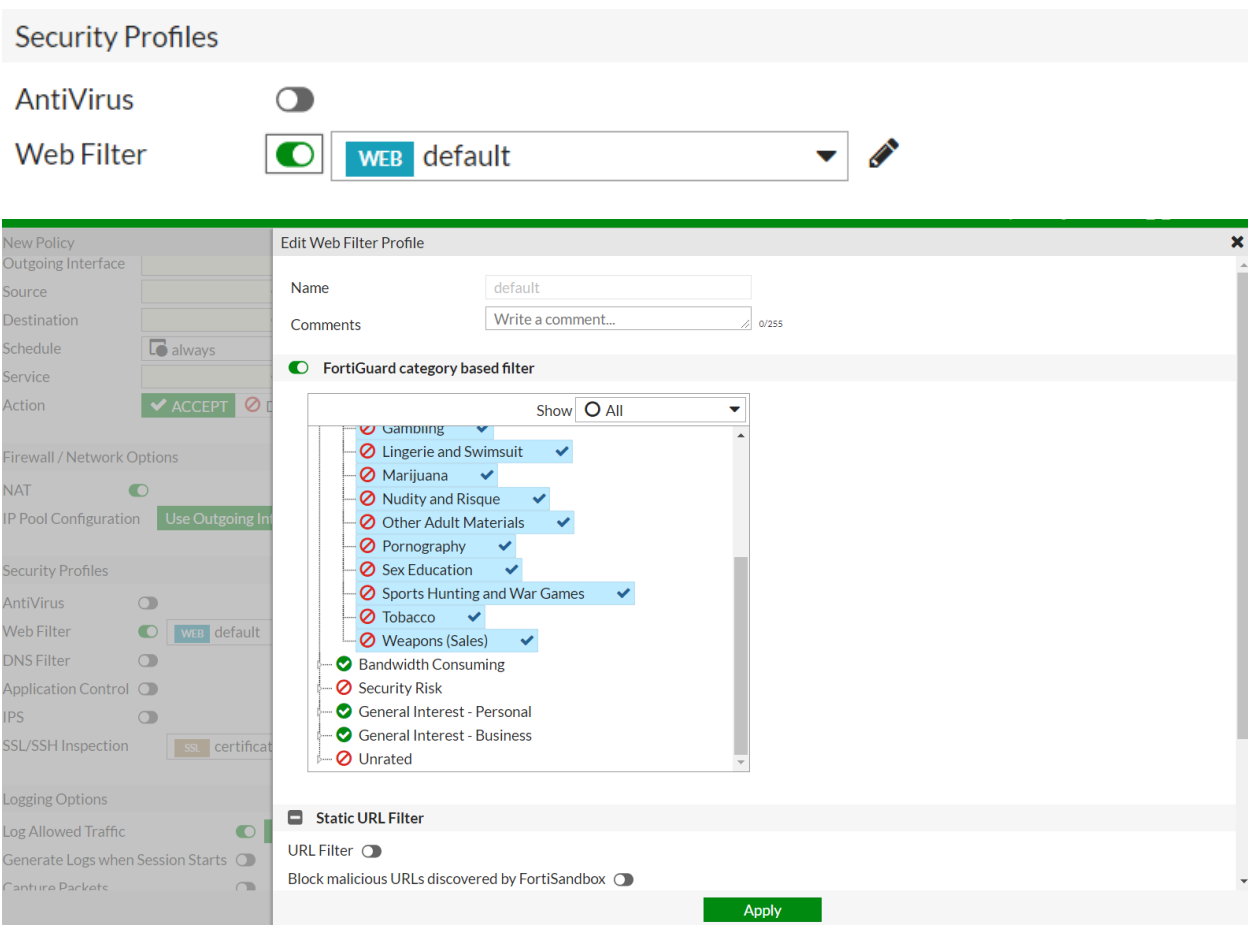
The screenshot shows the FortiGate VM64 Firewall configuration interface. The left sidebar contains a navigation menu with categories like Dashboard, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The 'Policy & Objects' section is expanded, and 'IPv4 Policy' is selected. The main area displays the 'New Policy' configuration form. The form includes fields for Name, Incoming Interface, Outgoing Interface, Source, Destination, Schedule, Service, and Action. The Action field has radio buttons for ACCEPT, DENY, and LEARN. Below these fields are sections for Firewall / Network Options (NAT, IP Pool Configuration) and Security Profiles (AntiVirus, Web Filter, DNS Filter, Application Control, IPS). The bottom of the form has OK and Cancel buttons.

This screenshot shows the 'New Policy' configuration form with specific values entered. The Name is 'Internet'. The Incoming Interface is 'LAN (port2)'. The Outgoing Interface is 'External (port1)'. The Source is 'all'. The Destination is 'all'. The Schedule is 'always'. The Service is 'ALL'. The Action is 'ACCEPT'. The Firewall / Network Options section shows NAT is enabled. The IP Pool Configuration section shows 'Use Outgoing Interface Address' is selected.

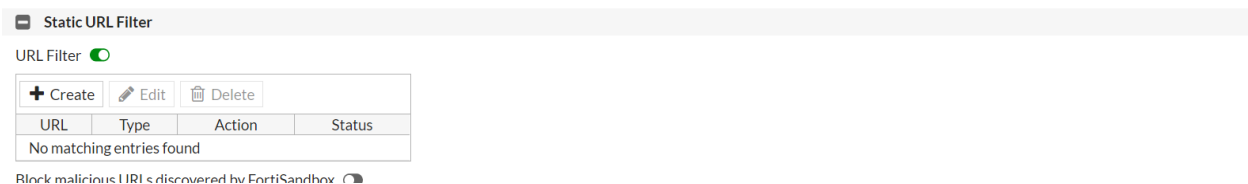
- Name: tên của Policy
- Incoming Interface: cổng mạng LAN muốn ra ngoài Internet
- Outgoing Interface: cổng mạng WAN để ra Internet
- Source: chọn All là tất cả hoặc tùy chọn
- Destination: chọn All là tất cả hoặc tùy chọn
- Service: chọn All là tất cả hoặc tùy chọn
- Phải bật chế độ NAT thành on

## b) Kiểm soát truy cập Web

- Tiếp tục ở mục trên bật chế độ Web Filter và nhấn vào biểu tượng cây viết để chỉnh sửa



- Muốn kiểm soát một URL thì ta phải bật URL Filter



- Sau đó vào Create để thêm => Điền địa chỉ trang web => Chọn option

New URL Filter

URL

Type **Simple** Reg. Expression Wildcard

Action Exempt **Block** Allow Monitor

Status ☒

OK Cancel

- Sau đó nhấn OK để thêm

Static URL Filter

URL Filter ☒

**+ Create** Edit Delete

URL	Type	Action	Status
http://gn.zing.vn/ga-bay-sinh-ton-2?utm_source=Ba...	Simple	Block	Enable

### c) Kiểm soát port truy cập

Vào mục Policy & Objects => Services => Hiện ra bảng các dịch vụ và port dùng để truy cập

FortiGate VM64 Firewall						
<div> <div>Dashboard</div> <div>FortiView</div> <div>Network</div> <div>System</div> <div>Policy &amp; Objects</div> <div>IPv4 Policy</div> <div>IPv4 DoS Policy</div> <div>Addresses</div> <div>Internet Service Database</div> <div>Services</div> <div>Schedules</div> <div>Virtual IPs</div> <div>IP Pools</div> <div>Traffic Shapers</div> <div>Traffic Shaping Policy</div> <div>Security Profiles</div> <div>VPN</div> <div>User &amp; Device</div> <div>WiFi &amp; Switch Controller</div> <div>Log &amp; Report</div> <div>Monitor</div> </div> <div> <div>Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> <div>Category Settings</div> <div>Search</div> <div>By Category</div> <div>Alphabetically</div> </div>						
Service Name	Category	Details	IP/FQDN	Show in Service List	Ref.	
General (4)						
ALL	General	ANY		<input checked="" type="checkbox"/>	1	
ALL_ICMP	General	ICMP/ANY		<input checked="" type="checkbox"/>	0	
ALL_TCP	General	TCP/1-65535	0.0.0.0	<input checked="" type="checkbox"/>	0	
ALL_UDP	General	UDP/1-65535	0.0.0.0	<input checked="" type="checkbox"/>	0	
Web Access (2)						
HTTP	Web Access	TCP/80	0.0.0.0	<input checked="" type="checkbox"/>	1	
HTTPS	Web Access	TCP/443	0.0.0.0	<input checked="" type="checkbox"/>	2	
File Access (8)						
AFS3	File Access	TCP/7000-7009 UDP/7000-7009	0.0.0.0	<input checked="" type="checkbox"/>	0	
FTP	File Access	TCP/21	0.0.0.0	<input checked="" type="checkbox"/>	0	
FTP_GET	File Access	TCP/21	0.0.0.0	<input checked="" type="checkbox"/>	0	
FTP_PUT	File Access	TCP/21	0.0.0.0	<input checked="" type="checkbox"/>	0	
NFS	File Access	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	<input checked="" type="checkbox"/>	0	
SAMBA	File Access	TCP/139	0.0.0.0	<input checked="" type="checkbox"/>	1	
SMB	File Access	TCP/445	0.0.0.0	<input checked="" type="checkbox"/>	1	
TFTP	File Access	UDP/69	0.0.0.0	<input checked="" type="checkbox"/>	0	
Email (6)						
IMAP	Email	TCP/143	0.0.0.0	<input checked="" type="checkbox"/>	1	
IMAPS	Email	TCP/993	0.0.0.0	<input checked="" type="checkbox"/>	1	
POP3	Email	TCP/110	0.0.0.0	<input checked="" type="checkbox"/>	1	

Ví dụ ta cấu hình cho một dịch vụ bằng cách nhấp đúp chuột vào dịch vụ đó

FortiGate VM64 Firewall						
<div> <div>Dashboard</div> <div>FortiView</div> <div>Network</div> <div>System</div> <div>Policy &amp; Objects</div> <div>IPv4 Policy</div> <div>IPv4 DoS Policy</div> <div>Addresses</div> <div>Internet Service Database</div> <div>Services</div> <div>Schedules</div> <div>Virtual IPs</div> <div>IP Pools</div> <div>Traffic Shapers</div> <div>Traffic Shaping Policy</div> <div>Security Profiles</div> <div>VPN</div> <div>User &amp; Device</div> <div>WiFi &amp; Switch Controller</div> <div>Log &amp; Report</div> <div>Monitor</div> </div> <div> <div>Edit Service</div> </div>						
<div> <div>Name</div> <div>HTTP</div> </div> <div> <div>Comments</div> <div></div> </div> <div> <div>Show in Service List</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Category</div> <div>Web Access</div> </div>						
Protocol Options						
<div> <div>Protocol Type</div> <div>TCP/UDP/SCTP</div> </div> <div> <div>Address</div> <div>IP Range FQDN 0.0.0.0</div> </div> <div> <div>Destination Port</div> <div>TCP 80 High</div> </div> <div> <div>Specify Source Ports</div> <div><input type="checkbox"/></div> </div>						
<div> <div>OK</div> <div>Cancel</div> </div>						

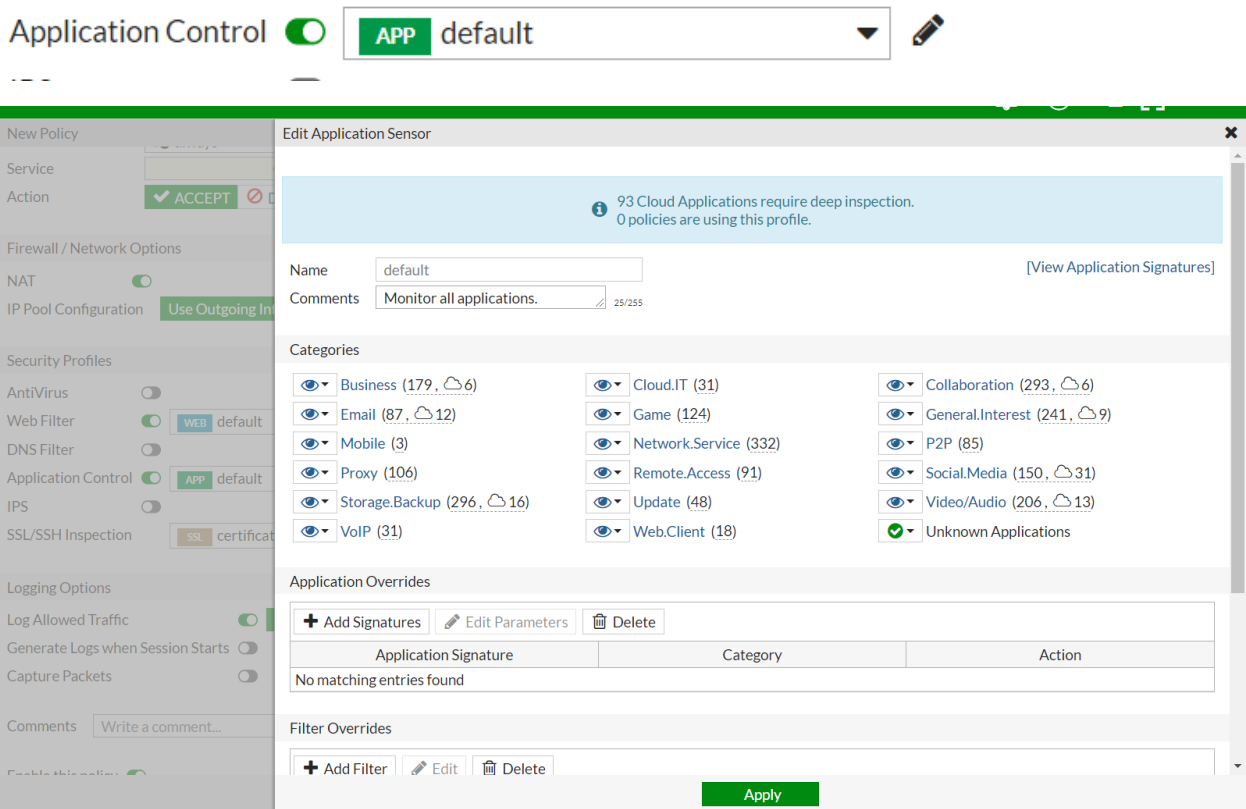
Ta có thể cấu hình các thông số như:

- Tên dịch vụ:
- Mục:
- Loại giao thức:
- Dải địa chỉ IP được phép truy cập:
- Port sử dụng
- ...



d) Kiểm soát ứng dụng truy cập

- Bật chế độ Application Filter và nhấn vào biểu tượng cây bút để chỉnh sửa



- Chọn mũi tên kế biểu tượng con mắt hiện ra các option sau:
  - + Allow
  - + Block
  - + Quarantine
  - + View Signatures
- Giờ chúng ta sẽ thử cấu hình kiểm soát một ứng dụng truy cập
  - Vào mục Application Overrides => Add Signatures => Chọn một ứng dụng trong bảng => Use Selected Signatures

Edit Application Sensor

Name

default

Comments

Monitor all applications.

Categories

Business (179, ☁ 6)

Game (124)

P2P (85)

Storage.Backup (296, ☁ 16)

Web.Client (18)

Application Overrides

+ Add Signatures

Edit Parameters

No matching entries found

Filter Overrides

+ Add Filter

Edit

Delete

No matching entries found

Options

Add Signatures

Select All

+ Add Filter

All

Cloud

Selected: 0 / 2414

Name	Category	Technology	Popularity	Risk
Zynga.Games	Game	Browser-Based	★★★★☆	■■■■■
Zyncro_Share.Attached.File	Social.Media	Browser-Based	★★★★☆	■■■■■
Zyncro	Social.Media	Browser-Based	★★★★☆	■■■■■
Zwiki	Collaboration	Browser-Based	★★★★☆	■■■■■
Zune	Video/Audio	Client-Server	★★★★☆	■■■■■
Zumodrive	Storage.Backup	Client-Server	★★★★☆	■■■■■
Zoosk	Social.Media	Browser-Based	★★★★☆	■■■■■
Zoom	Collaboration	Browser-Based, Client-Server	★★★★☆	■■■■■
Zoho_Login	Business	Browser-Based	★★★★☆	■■■■■
Zoho_File.Upload	Business	Browser-Based	★★★★☆	■■■■■
Zoho_File.Download	Business	Browser-Based	★★★★☆	■■■■■
Zoho.Wiki	Collaboration	Browser-Based	★★★★☆	■■■■■
Zoho.Sites_File.Upload	Business	Browser-Based	★★★★☆	■■■■■
Zoho.Sites	Business	Browser-Based	★★★★☆	■■■■■
Zoho.Show	Collaboration	Browser-Based	★★★★☆	■■■■■
Zoho.Reports	Business	Browser-Based	★★★★☆	■■■■■
Zoho.Projects	Business	Browser-Based	★★★★☆	■■■■■
Zoho.People	Business	Browser-Based	★★★★☆	■■■■■
Zoho.Notebook	General.Interest	Browser-Based	★★★★☆	■■■■■
Zoho.Meeting	Collaboration	Browser-Based	★★★★☆	■■■■■
Zoho.Mail	Email	Browser-Based	★★★★☆	■■■■■
Zoho.CRM	Business	Browser-Based	★★★★☆	■■■■■

<<

<

1

>

>>

[Total: 2414]

Use Selected Signatures

Cancel

- Ứng dụng được chọn đã hiện lên trong bảng

Application Overrides

+ Add Signatures

Edit Parameters

Delete

Application Signature	Category	Action
Zynga.Games	Game	Block

- Có các option để chúng ta lựa chọn

Application Overrides

+ Add Signatures

Edit Parameters

Delete

Application Signature	Category	Action
Zynga.Games	Game	<div> <div>Block</div> <div>Monitor</div> <div>Allow</div> <div>Block</div> <div>Quarantine</div> </div>

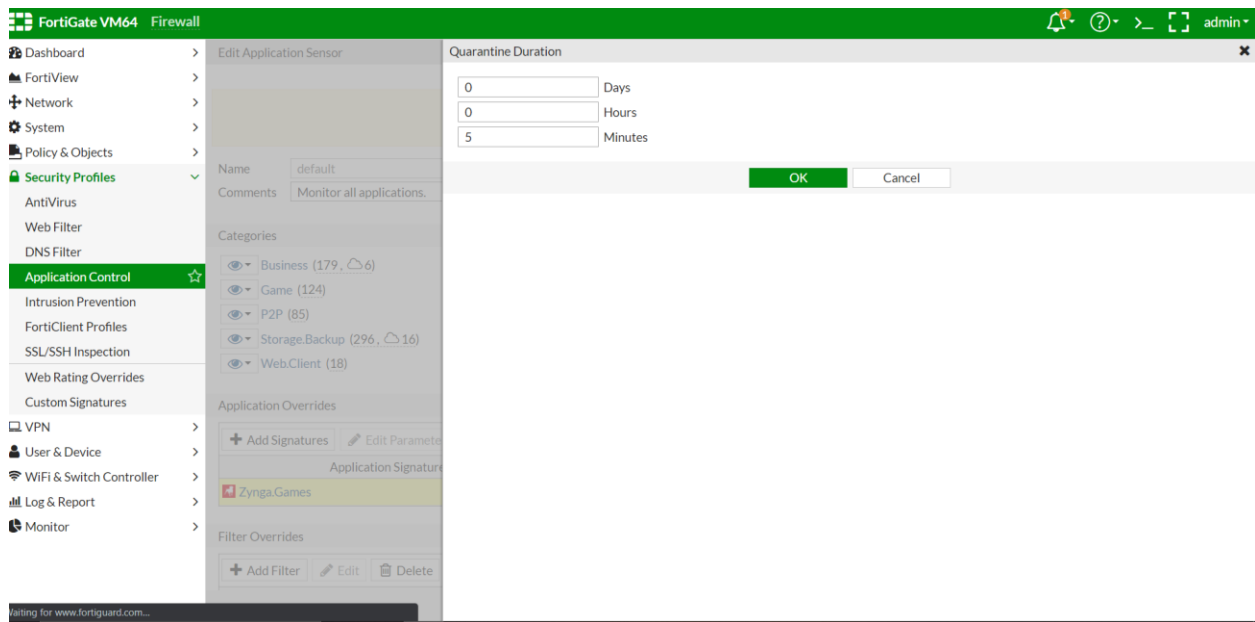
Filter Overrides

+ Add Filter

Edit

Delete

- Chọn option Quarantine để cài đặt thời gian



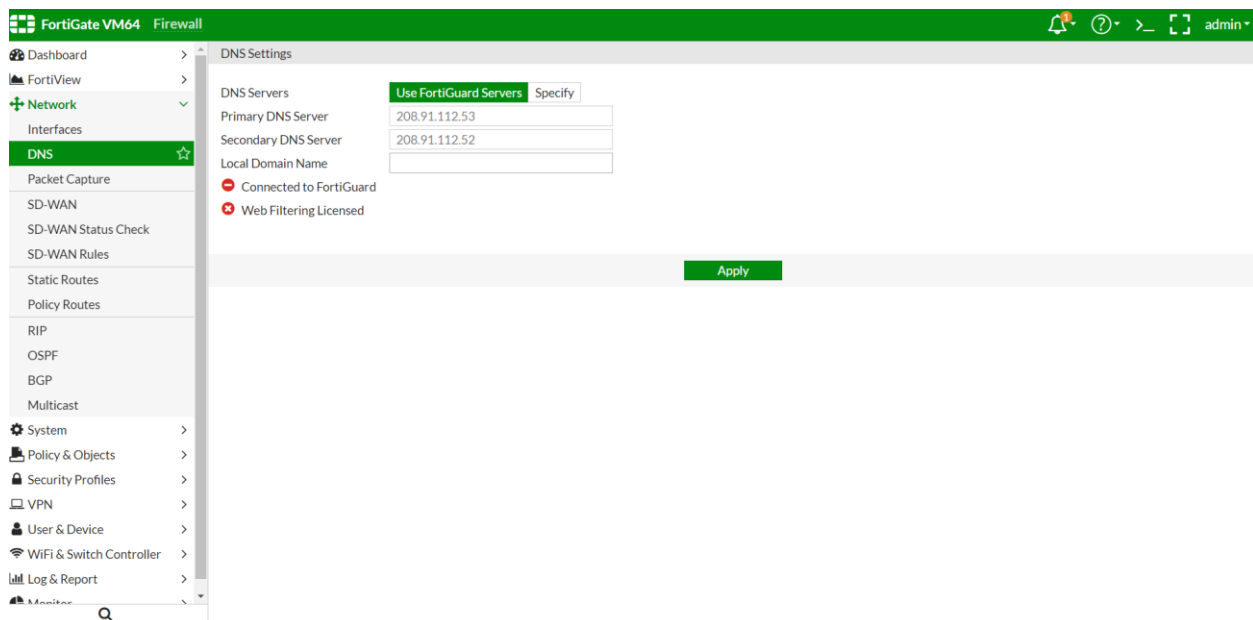
- Set thời gian thành công

Application Overrides

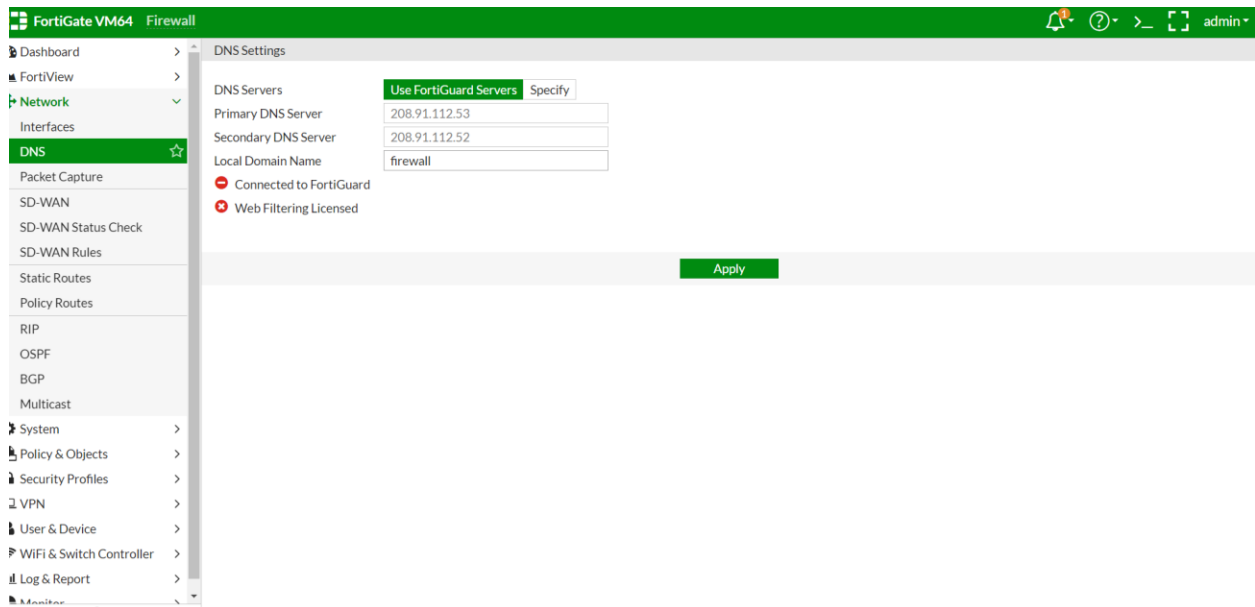
<a href="#">+ Add Signatures</a>	<a href="#">Edit Parameters</a>	<a href="#">Delete</a>
Application Signature	Category	Action
Zynga.Games	Game	<a href="#">Quarantine</a> Expires 5 Minute(s)

e) Thực hiện các phương thức khác : DNS

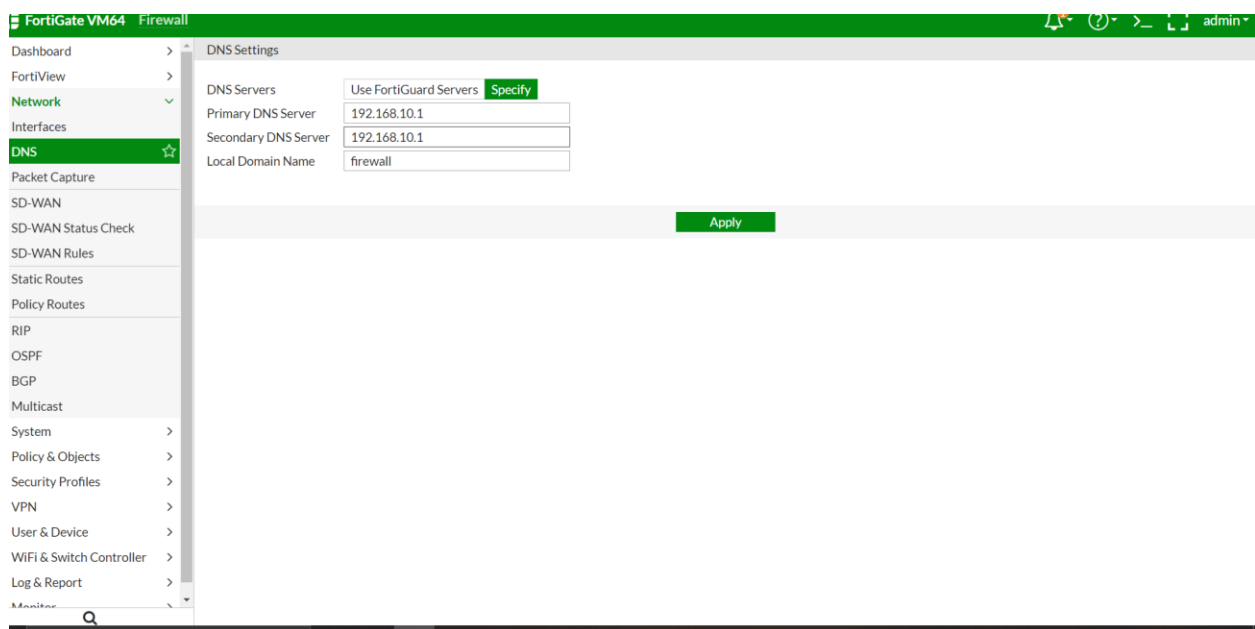
Vào mục Network => DNS => Hiện ra bảng gồm 2 option



- Nếu chọn DNS mặc định thì điền tên Domain vào bảng



- Hoặc nếu tự cấu hình DNS riêng



#### 4. Snort-IDS

- Tải phần mềm Snort trên trang chủ <https://snort.org/downloads>
- Cài đặt phần mềm Snort vào máy
- Cài đặt phần mềm WinPcap
- Vào Command Line => gõ `cd \Snort\bin => snort -V` để kiểm tra phần mềm đã cài đặt thành công chưa và phiên bản

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.1198]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\darks>cd \Snort\bin

C:\Snort\bin>snort -V

  __ _
 o"  )~
  ' ' '

-*> Snort! <*-
Version 2.9.17-WIN32 GRE (Build 199)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

C:\Snort\bin>
```

•

## 5. Network Monitoring System

5.1 Tải và cài đặt công cụ PRTG trên trang chủ

5.2 Sau khi cài đặt thành công thì giao diện của công cụ như dưới đây