



## CẤU HÌNH CÁC TÍNH NĂNG FORTIGATE

Môi trường: Lab ảo eve-ng

**Hãy share tài liệu cho những người mới cùng học**

Người viết: HaiNguyen-IT

Join nhóm CCNA: [bit.ly/lab-network](https://bit.ly/lab-network)

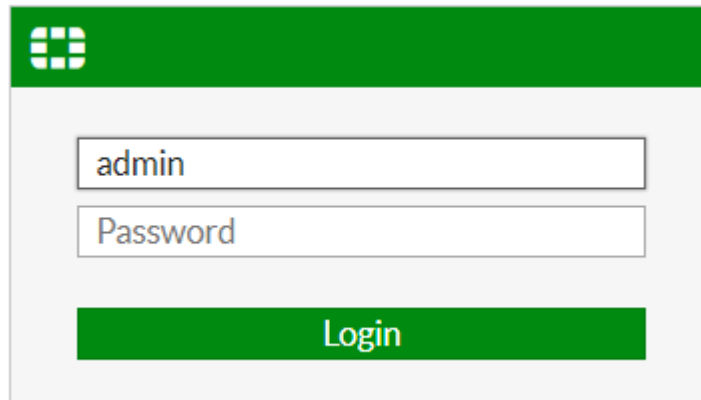
## **Mục Lục**

- 1. Vào web gui của tường lửa**
- 2. Backup-Restore cấu hình**
- 3. Check version software/ Upgrade software**
- 4. Cấu hình NAT đi internet**
- 5. Mở port FTP/HTTP server**
- 6. Chống tấn công DoS**
- 7. Lọc website có hại**
- 8. Chặn file chứa virus**
- 9. Chống rò rỉ dữ liệu nhạy cảm DLP**
- 10. Cấu hình deep-inspect traffic**
- 11. VPN giữa 2 Fortigate**
- 12. Hai tường lửa dự phòng (node, link)**
- 13. Cấu hình dự phòng wan internet**
- 14. Cấu hình IPS**
- 15. Giám sát log người dùng**
- 16. Bóp băng thông**

### **1. Vào web gui của tường lửa**

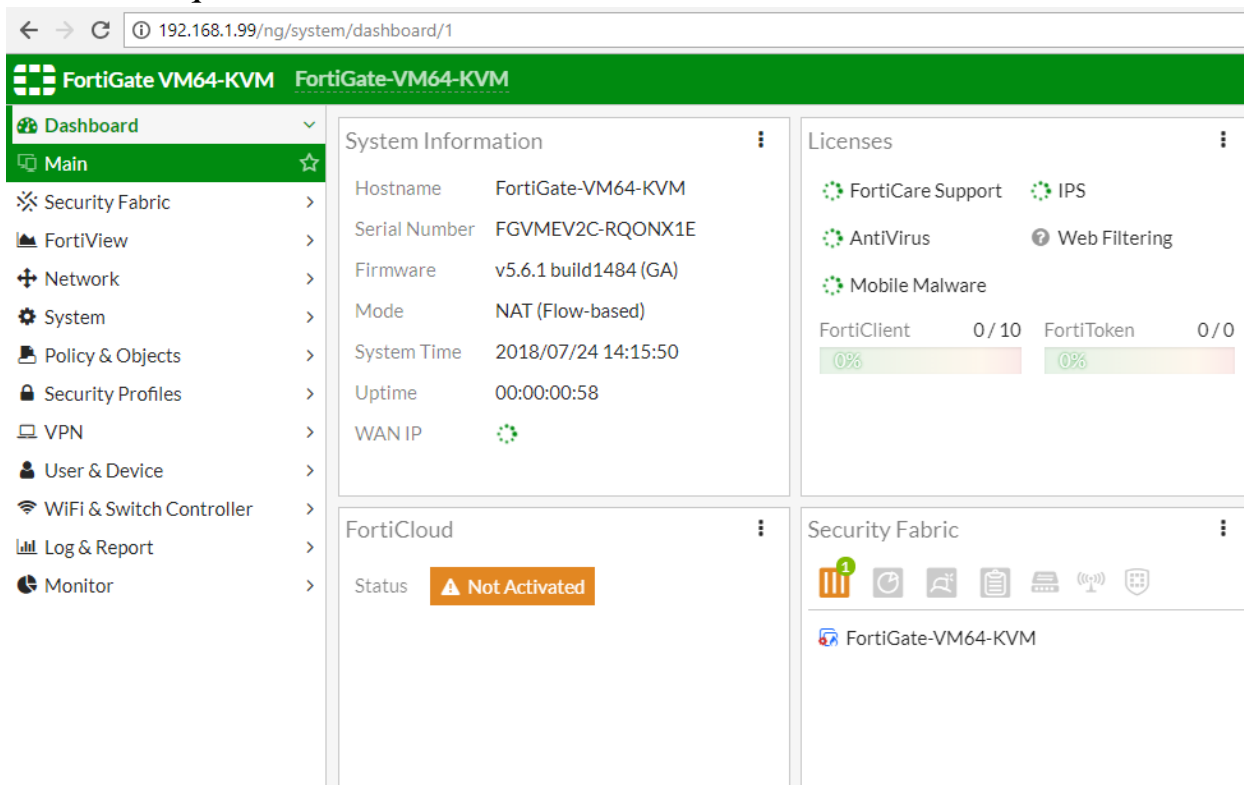
- Đặt IP cho máy tính là 192.168.1.100/24

- Connect máy tính vào port 1 của Fortigate (địa chỉ port này thường để mặc định là 192.168.1.99) .Nếu chưa có thì đặt IP này cho port 1. Gõ <https://192.168.1.99>. Nếu bị lỗi SSL thì xóa history và đợi 1 lúc vào lại, hoặc google tìm cách sửa.



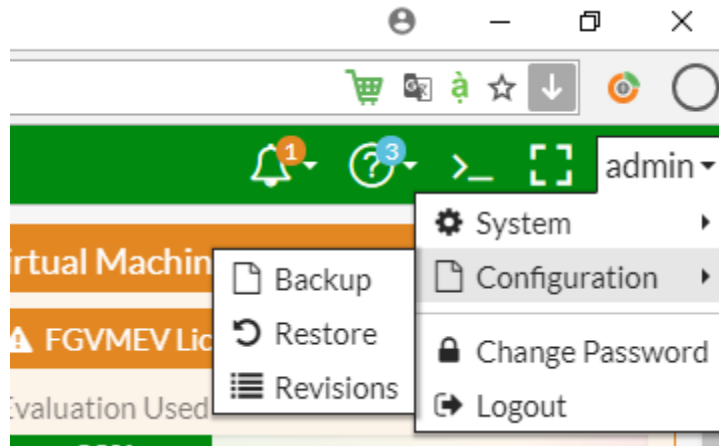
Tài khoản: admin/ không có password

- Kết quả như hình:



## 2. Backup-Restore cấu hình

- Vào admin chọn 1 trong 2 lựa chọn như hình

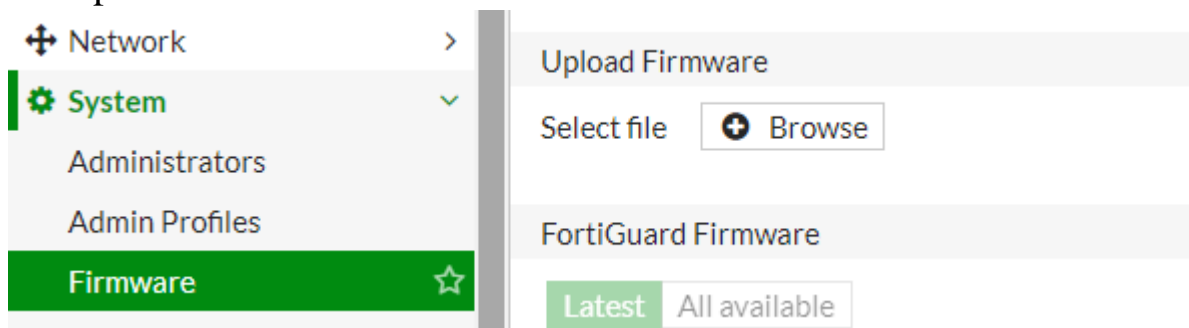


### 3. Check version software và Upgrade như nào

- Version của software như hình

System Information	
Hostname	FortiGate-VM64-KVM
Serial Number	FGVMEV2C-RQONX1E
Firmware	v5.6.1 build1484 (GA)

- Để upgrade firmware: vào system-> Firmware, chọn Browser đến file cần update.

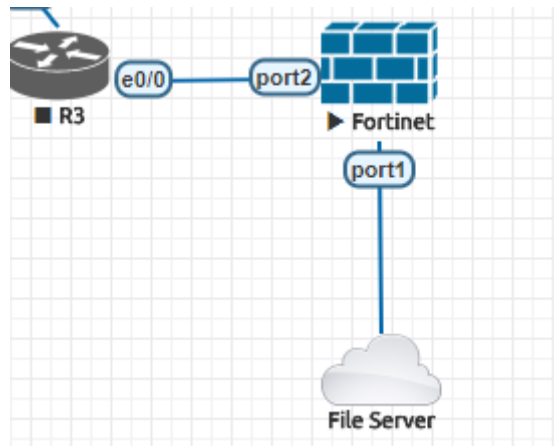


Tham khảo thêm ở link sau

<https://cookbook.fortinet.com/updating-your-fortigates-firmware-54/>

### 4. Cấu hình NAT đi internet

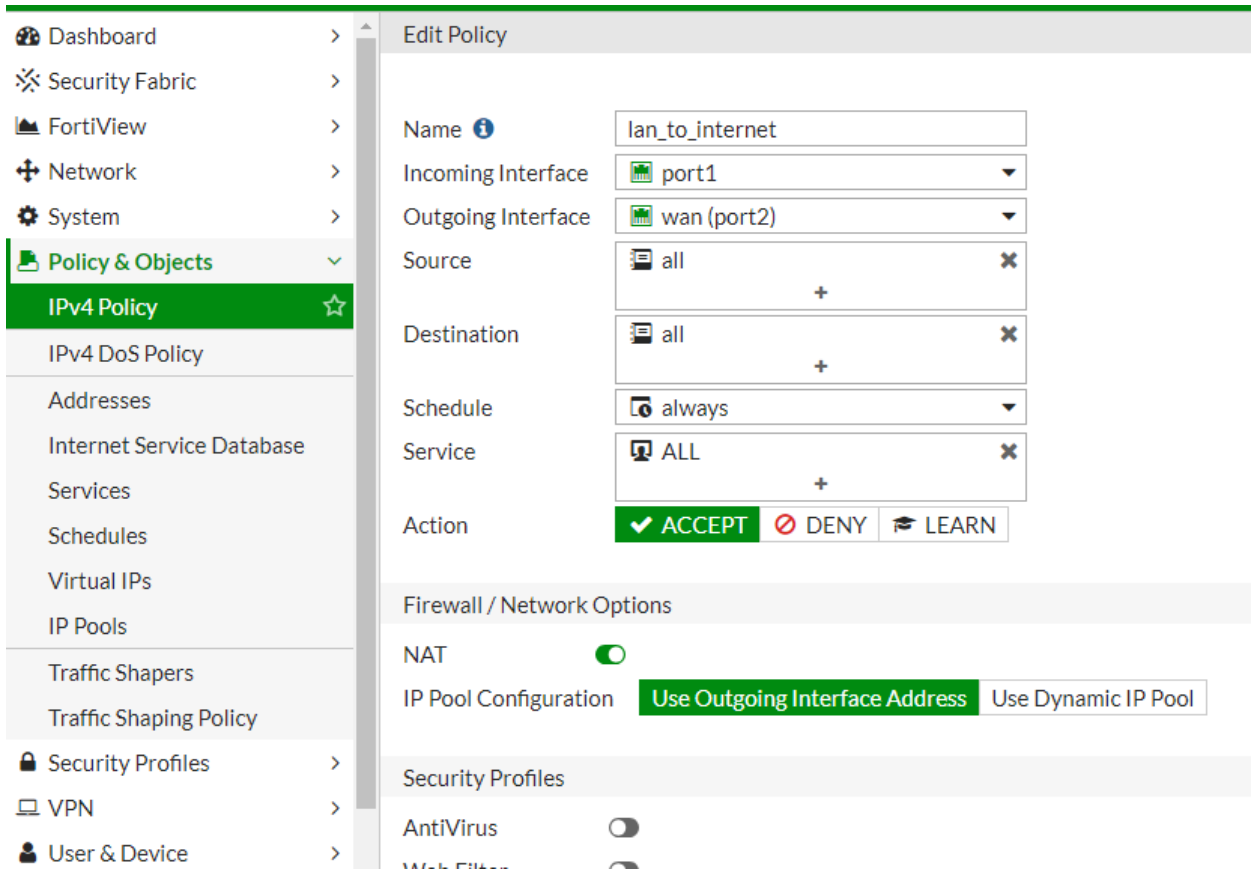
Mô hình



- Check đã cấu hình IP cho interface, port 1 nối tới máy tính LAN, port 2 nối đến internet

Name	Members	IP/Netmask
<a href="#">port1</a>		192.168.1.99 255.255.255.0
<a href="#">port2 (wan)</a>		10.3.4.4 255.255.255.0
<a href="#">port3</a>		0.0.0.0 0.0.0.0
<a href="#">port4</a>		0.0.0.0 0.0.0.0

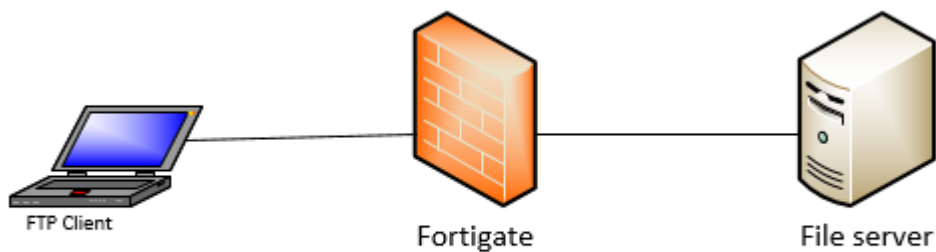
- Vào Policy&Object tạo policy để cho ra internet, nhớ chọn NAT



- Check lại: từ Máy tính trong LAN, ping ra ngoài google hoặc 8.8.8.8 ok

## 5. Cấu hình mở port FTP/HTTP server

- Mô hình



- Vào interface, ghi lại IP wan

	port2 (wan)	10.3.4.4 255.255.255.0
--	-------------	------------------------

- Vào Virtual IP → gõ IP WAN /LAN như bên dưới

FortiView > Edit Virtual IP

Name: FTP-Server  
Comments:   
Color: [Change]

Network

Interface: wan (port2) **IP wan**

Type: Static NAT

External IP Address/Range: 10.3.4.4 - 10.3.4.4

Mapped IP Address/Range: 192.168.1.100 - 192.168.1.100 **IP LAN của File server**

Optional Filters:

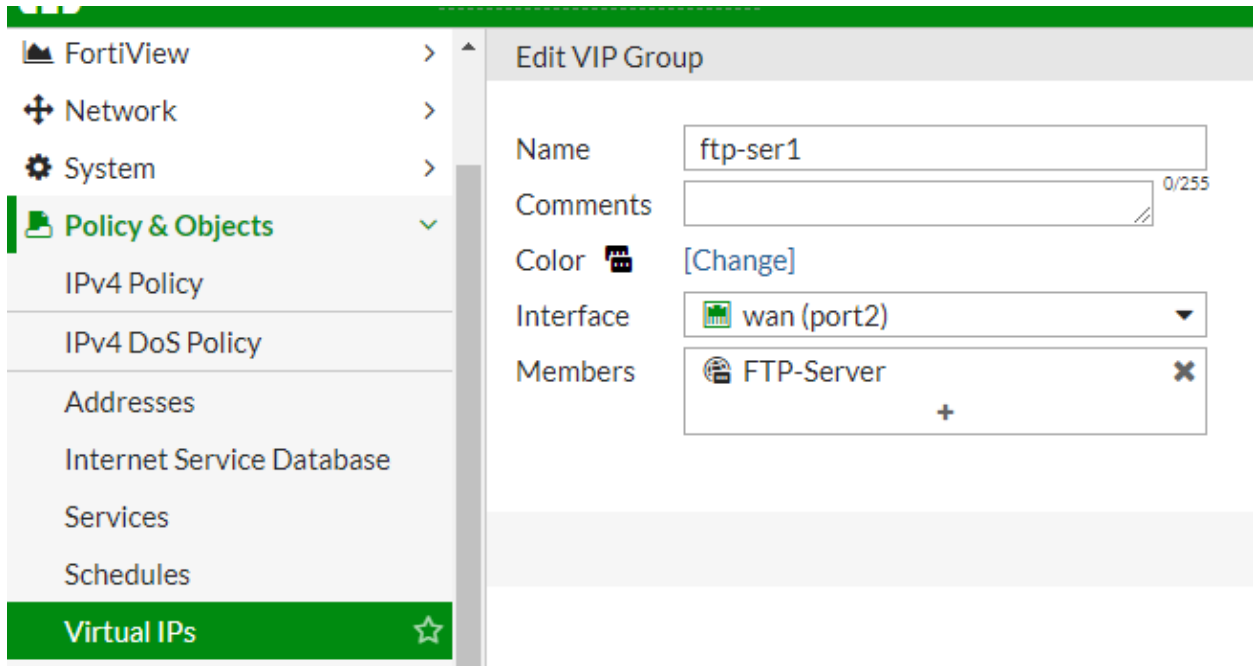
Port Forwarding:

Protocol: **TCP** | UDP | SCTP | ICMP **Chọn 21**

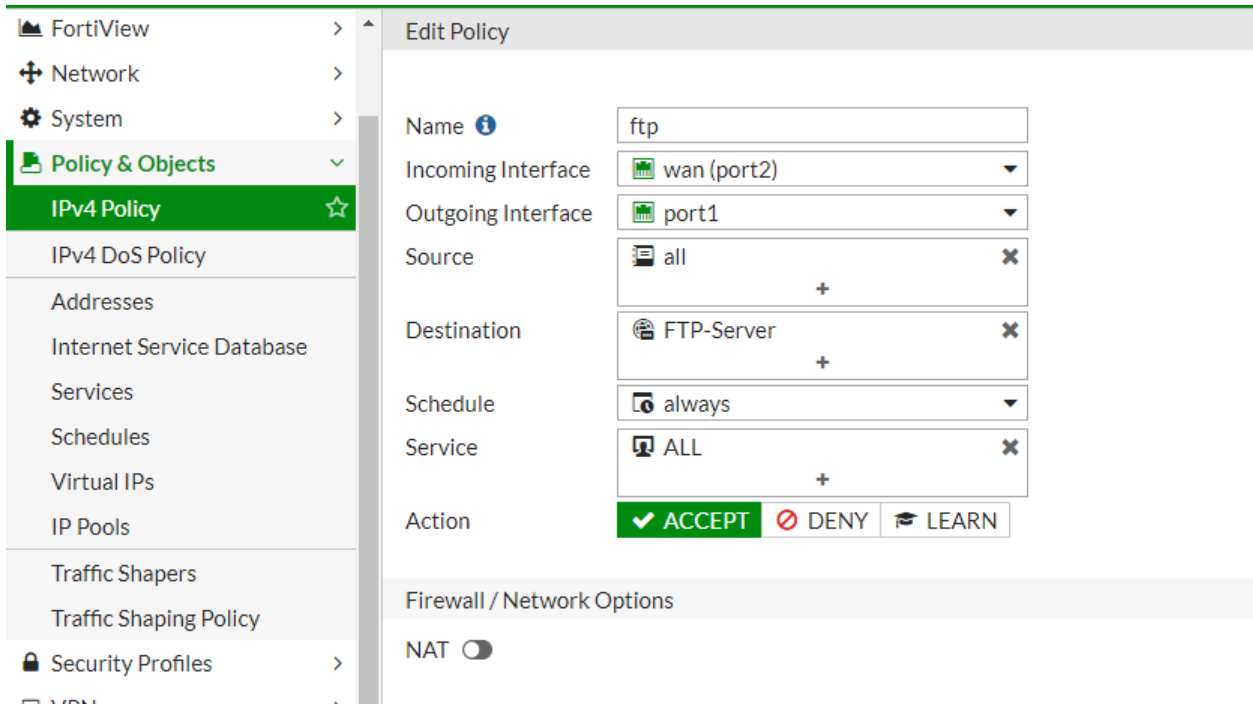
External Service Port: 21 - 21

Map to Port: 21 - 21

- Vào virtual IP → Create new → Virtual IP group, điền như dưới



- Vào Policy&Object ->IPv4 Policy →Create new, chọn như hình , **chú ý NAT off**



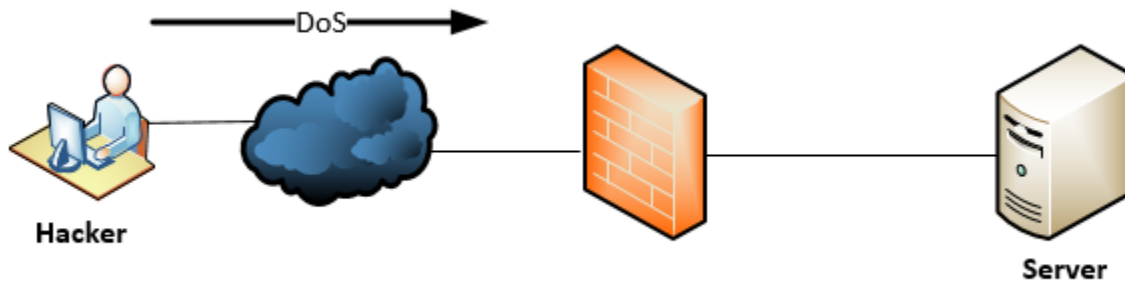
- Dùng Filezilla để test kết quả

Mở port HTTP tương tự



## 6. Chống tấn công DoS

- Mô hình:



- Kịch bản: Hacker dùng icmp ping liên tục tới server
- Phương án: Đo xem trong 1 khoảng thời gian (ví dụ 1s) có  $\geq 250$  gói ping từ 1 IP thì sẽ block/drop các gói tin đó

Vào **Policy & Object** → **IPv4 DoS Policy**

Field	Value
Incoming Interface	wan (port2)
Source Address	all
Destination Address	all
Services	ALL

Chọn incoming interface là WAN

Chỉ ra source address/destination address cần giám sát

Loại service cần bảo vệ

Có nhiều loại thông số để làm thước đo tấn công DoS

### L3 Anomalies

Name	<input type="checkbox"/> Status	<input type="checkbox"/> Logging	Pass <input checked="" type="checkbox"/> Block Action	Threshold
ip_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass <input checked="" type="checkbox"/> Block	2
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass <input checked="" type="checkbox"/> Block	2

### L4 Anomalies

Name	<input type="checkbox"/> Status	<input checked="" type="checkbox"/> Logging	Pass <input type="checkbox"/> Block Action	Threshold
tcp_syn_flood	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Pass <input type="checkbox"/> Block	2000
tcp_port_scan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Pass <input type="checkbox"/> Block	1000
tcp_src_session	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass <input checked="" type="checkbox"/> Block	1
tcp_dst_session	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Pass <input type="checkbox"/> Block	5000
udp_flood	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Pass <input type="checkbox"/> Block	2000
udp_scan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Pass <input type="checkbox"/> Block	2000

Ý nghĩa các thông số tham khảo ở link

<http://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Security%20Policies/DoS%20Protection.htm>

Khi bật 1 thông số nào đó thì ta cần enable Status

icmp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass <input checked="" type="checkbox"/> Block	250
------------	-------------------------------------	-------------------------------------	--	-----

Ví dụ như trên là enable bộ đếm ping


- Verify: Dùng nhiều cửa sổ ping (hoặc chỉnh ngưỡng đo còn 2 gói/giây) ; nếu quá 250 gói/s thì các gói ping sẽ bị timeout/drop nhiều, khi ta tắt bộ đếm thì ping lại mượt.

## 7. Lọc web độc hại

### Block lẻ từng trang(cách cùi nhất)

- Step 1: đảm bảo đã có internet về máy user



port1 - To internet (port3) (1 - 1)							
1	lan_to_internet	all	all	always	ALL	✓ ACCEPT	✓ Enabled

- Step 2: Tạo 1 bộ lọc web filter:  
Nhấn dấu  góc trên bên phải

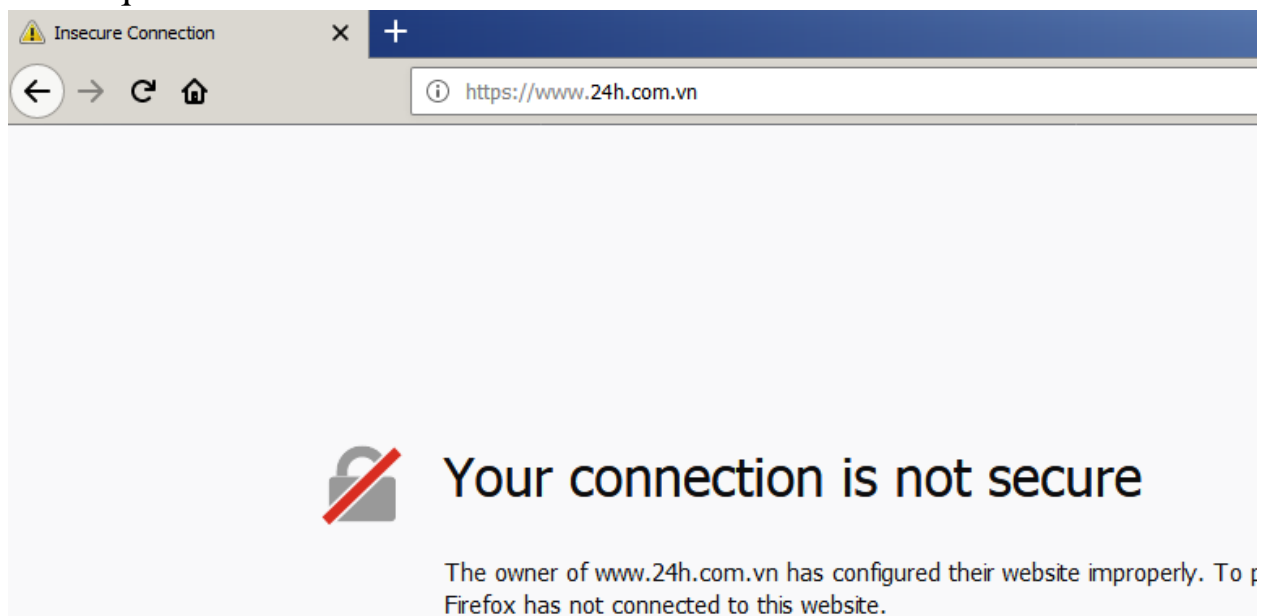


Tạo URL filter như này để block 24h.com.vn

URL Filter

URL	Type	Action	Status
*24h.com.vn	Wildcard	 Block	 Enable

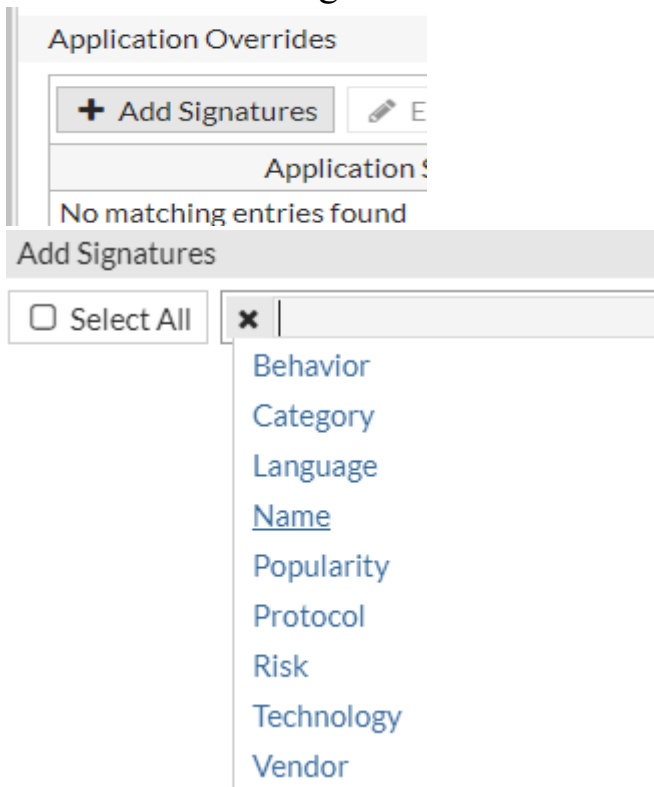
Kết quả:



(\*) Note: Để block được facebook, cần enable thêm Application control



Sau đó click Add signatures



Chọn name; gõ facebook

Add Signatures		
<input type="checkbox"/> Select All	<input checked="" type="checkbox"/> Name: Facebook	<input type="button" value="Add Filter"/>
Name	Category	Technology
Facebook	Social.Media	Browser-Based
Facebook.App	Social.Media	Browser-Based
Facebook.App_AngryBirds	Game	Browser-Based
Facebook.App_AvengersAlliance	Game	Browser-Based
Facebook.App_Bubble.Fairyland	Game	Browser-Based
Facebook.App_BubbleSafari	Game	Browser-Based
Facebook.App_CandyCrushSaga	Game	Browser-Based
Facebook.App_CastleVille	Social.Media	Browser-Based
Facebook.App_CityVille	Social.Media	Browser-Based
Facebook.App_Criminalcase	Game	Browser-Based
Facebook.App_EmpiresAndAllies	Game	Browser-Based
Facebook.App_Happyland	Game	Browser-Based
Facebook.App_IAMPlayr	Game	Browser-Based
Facebook.App_Kongregate	Social.Media	Browser-Based
Facebook.App_MafiaWars	Game	Browser-Based
Facebook.App_Miscrits	Game	Browser-Based
Facebook.App_MyTribe	Social.Media	Browser-Based
Facebook.App_Name	Social.Media	Browser-Based

Use Selected Signatures

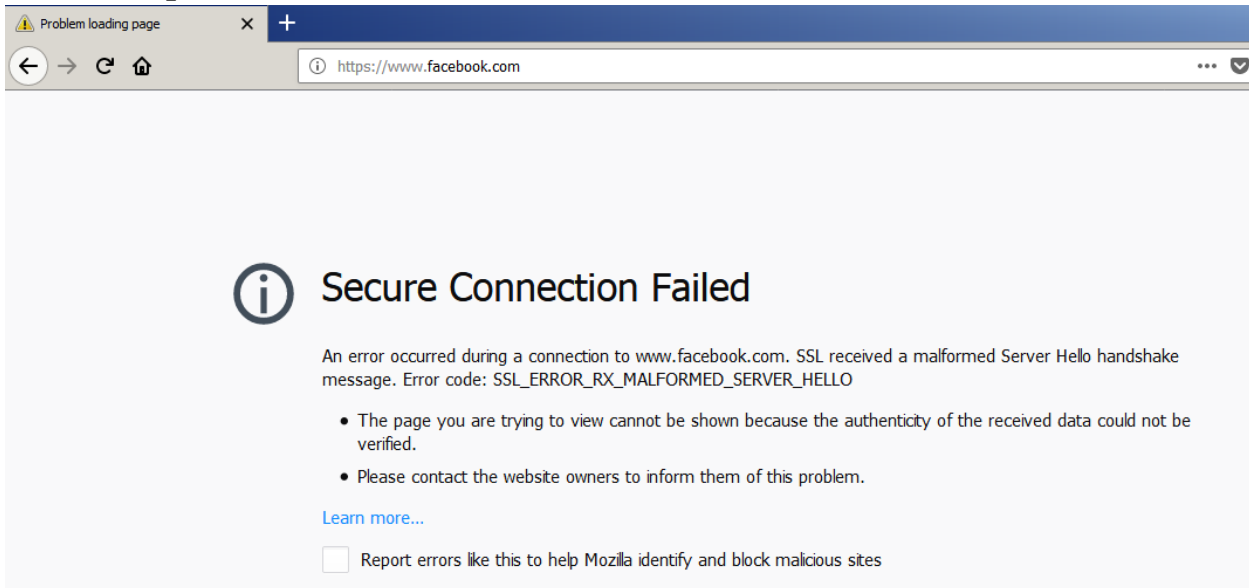
Bôi tất cả các dòng Facebook, Chọn

- Vào Policy; chọn edit Policy đi internet, chọn Application Control và SSL/SSH inspection như hình (nếu chọn deep-inspection thì all https bị die)

#### Security Profiles

AntiVirus	<input type="checkbox"/>		
Web Filter	<input checked="" type="checkbox"/>	WEB blockFB	
DNS Filter	<input type="checkbox"/>		
Application Control	<input checked="" type="checkbox"/>	APP default	
IPS	<input type="checkbox"/>		
SSL/SSH Inspection	<input type="checkbox"/>	SSL certificate-inspection	

## Kết quả

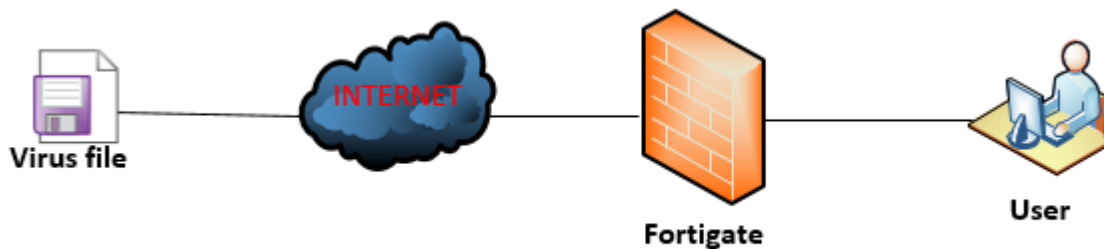


Block theo content(làm nhưng không chặn được)

### 8. Chặn file chứa virus

#### Chặn HTTP:

Dùng file **eicar** để test: khi bật antivirus thì không down được; bỏ bật thì down ok



Vào Security Proxy → Antivirus, tạo 1 profile AV mới

The screenshot shows the configuration page for a new Antivirus profile named 'testAV'. The left sidebar is expanded to 'Security Profiles' > 'Antivirus'. The main content area includes:

- Name:** testAV
- Comments:** Write a comment... (0/255)
- Detect Viruses:** Block (selected), Monitor
- Inspected Protocols:** HTTP, SMTP, POP3, IMAP, MAPI, FTP (all enabled).
- Inspection Options:** Treat Windows Executables in Email Attachments as Viruses (enabled), Include Mobile Malware Protection (enabled).

Vào policy để thêm AV profile:

The screenshot shows the configuration page for an IPv4 Policy named 'Edit Policy'. The left sidebar is expanded to 'Policy & Objects' > 'IPv4 Policy'. The main content area includes:

- Action:** ACCEPT (selected), DENY, LEARN
- Firewall / Network Options:** NAT (enabled), IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP F
- Security Profiles:** AntiVirus (enabled) with profile 'testAV' selected, Web Filter (disabled), DNS Filter (disabled), Application Control (disabled).

Vào máy tính download thử file EICAR,  
<http://www.eicar.org/85-0-Download.html>

Download area using the standard protocol http			
<a href="#">eicar.com</a>	<a href="#">eicar.com.txt</a>	<a href="#">eicar_com.zip</a>	<a href="#">eicarcom2.zip</a>
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Download area using the secure, SSL enabled protocol https			
<a href="#">eicar.com</a>	<a href="#">eicar.com.txt</a>	<a href="#">eicar_com.zip</a>	<a href="#">eicarcom2.zip</a>
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Kết quả bị block:

**High Security Alert!!**

You are not permitted to download the file "eicar.com.txt" because it is infected with the virus "EICAR\_TEST\_FILE".

URL: <http://www.eicar.org/download%2Feicar.com.txt>  
File quarantined as: [disabled].

[http://www.fortinet.com/ve?vn=EICAR\\_TEST\\_FILE](http://www.fortinet.com/ve?vn=EICAR_TEST_FILE)  
Client IP: 192.168.1.100  
Server IP: 213.211.198.62  
User name:  
Group name:

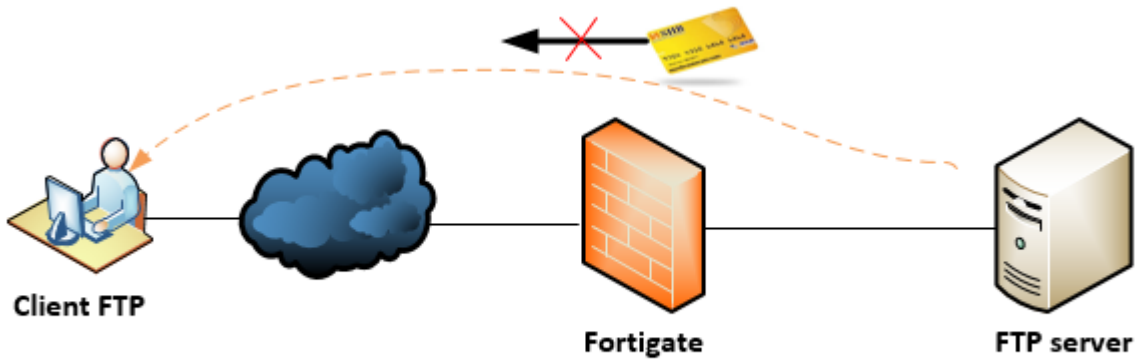
Nếu bỏ AV đi thì download OK



**Chặn HTTPS: đã enable SSL deep-inspection + AV nhưng vẫn ko được.  
Có thể do phiên bản trên VM không hỗ trợ**

## 9. Chống rò rỉ dữ liệu nhạy cảm DLP

Mô hình

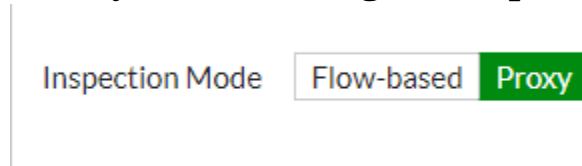


Kịch bản: Client download thông tin nhạy cảm , sẽ bị chặn

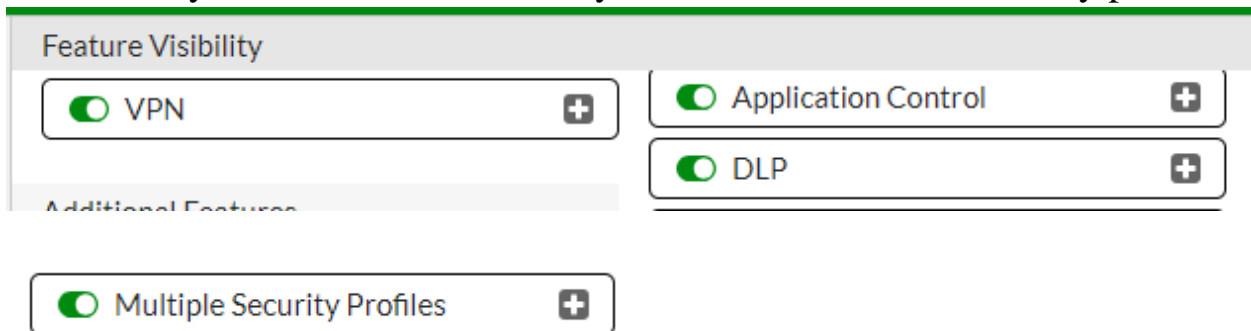
Thực hiện:

- Enable proxy-based

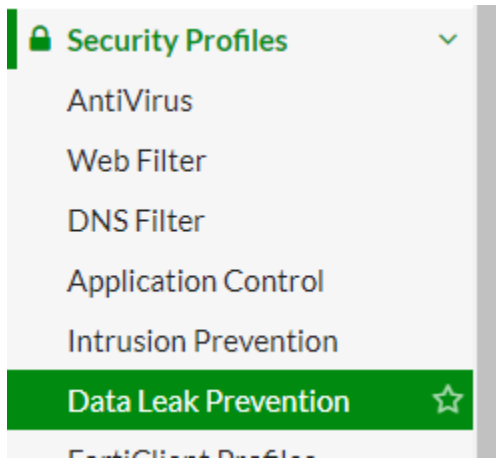
Vào **System** → **Settings** → **Inspection mode**



- Vào **System** → **Feature Visibility** → **Bật DLP và Multi security profile**



Vào Security Profile → Chọn DLP



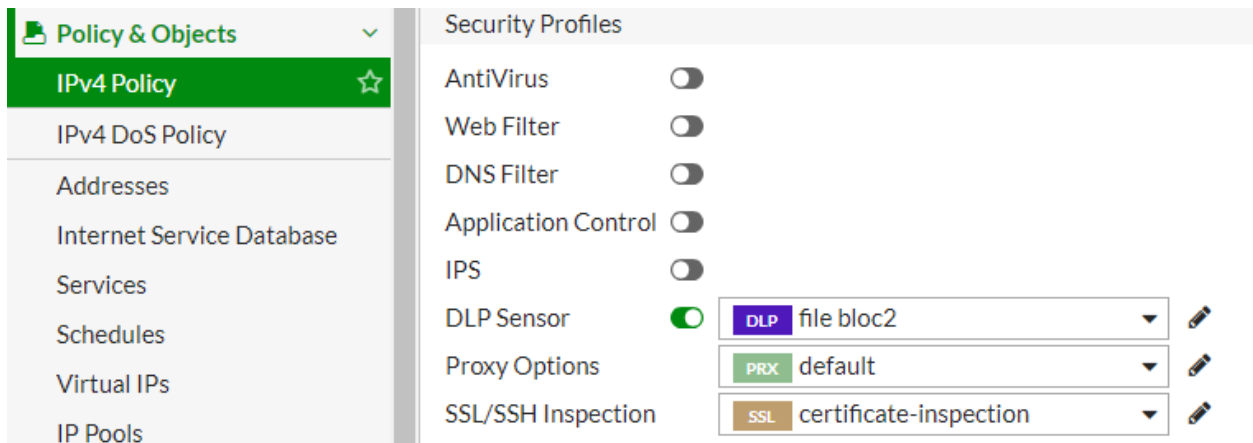
Vào chọn create new



Điền: type, action,...

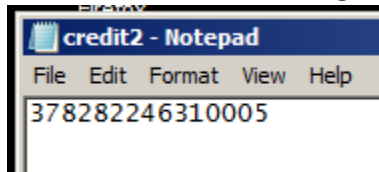
A screenshot of the 'Edit Filter' dialog box. The dialog has a title bar 'Edit Filter' with a close button. The main content is divided into several sections: 'Filter' with a 'Type' dropdown set to 'Files' and a search term 'Credit Card #'; 'Examine the Following Services' with checkboxes for 'Web Access' (HTTP-POST, HTTP-GET), 'Email' (SMTP, POP3, IMAP, MAPI), and 'Others' (FTP, NNTP); and 'Action' with a dropdown set to 'Log Only'. At the bottom are 'OK' and 'Cancel' buttons.

Vào **Policy & Object** → **IPv4 Policy**, chọn Policy muốn apply  
Apply DLP

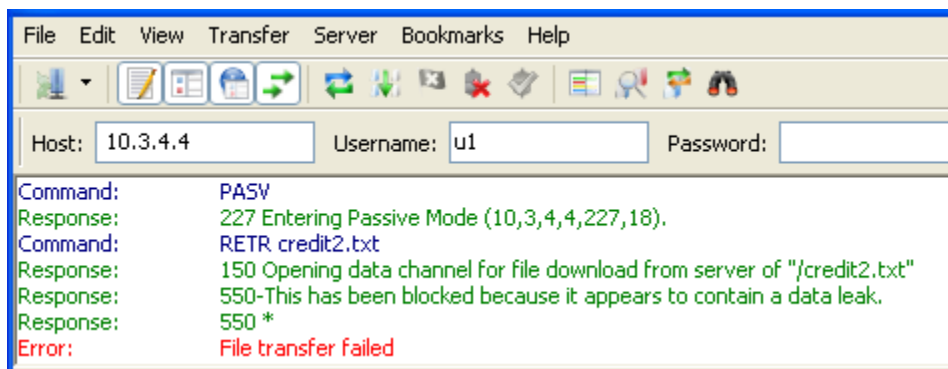


## Kết quả với FTP

Block file chứa thông tin thẻ tín dụng

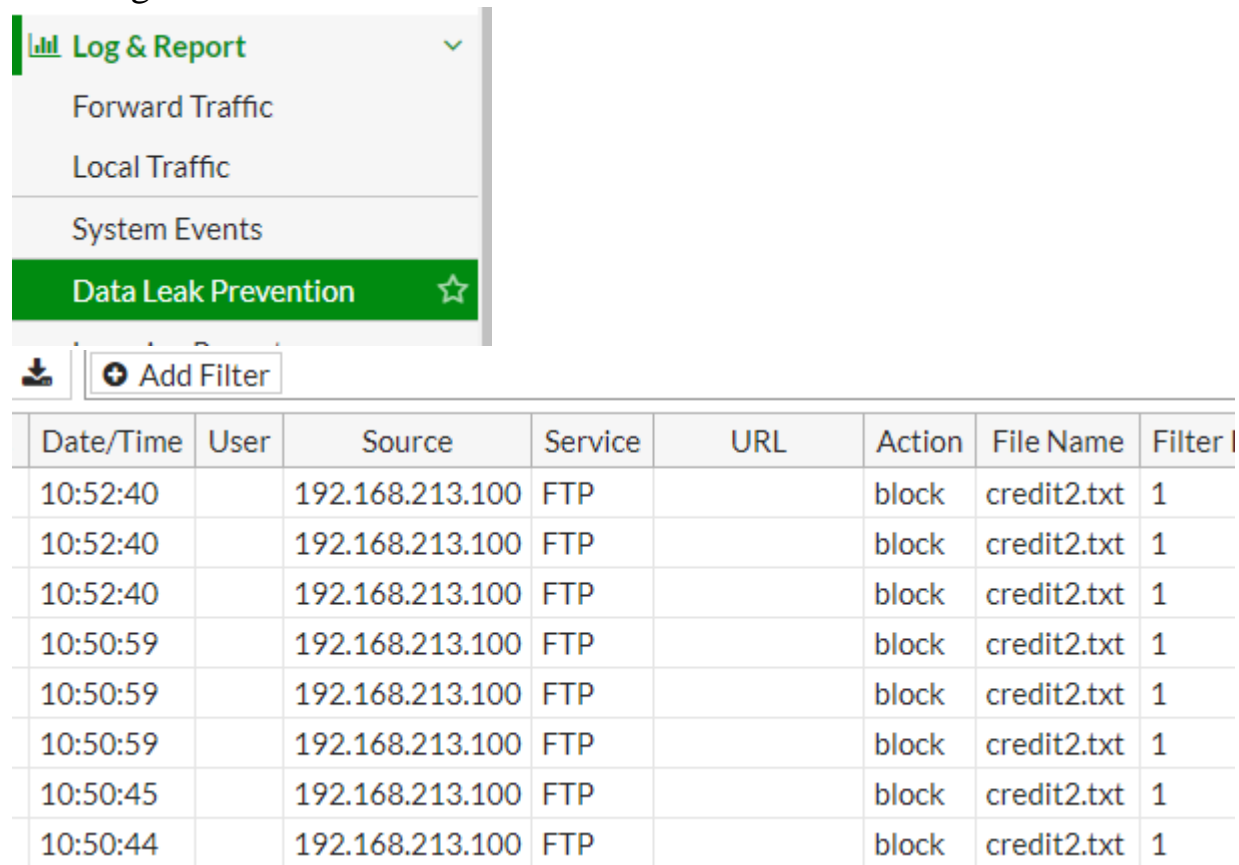


Download file này sẽ bị block



Download file khác thì ok

Xem log



Date/Time	User	Source	Service	URL	Action	File Name	Filter I
10:52:40		192.168.213.100	FTP		block	credit2.txt	1
10:52:40		192.168.213.100	FTP		block	credit2.txt	1
10:52:40		192.168.213.100	FTP		block	credit2.txt	1
10:50:59		192.168.213.100	FTP		block	credit2.txt	1
10:50:59		192.168.213.100	FTP		block	credit2.txt	1
10:50:59		192.168.213.100	FTP		block	credit2.txt	1
10:50:45		192.168.213.100	FTP		block	credit2.txt	1
10:50:44		192.168.213.100	FTP		block	credit2.txt	1

## 10. Cấu hình deep-inspect traffic

Mục đích: kiểm tra nội dung gói tin đã được mã hóa SSL

Cách thực hiện: Fortigate mở 1 phiên SSL tới Webserver rồi nhận content về; sau đó check content nếu ok thì chuyển lại cho UserPC

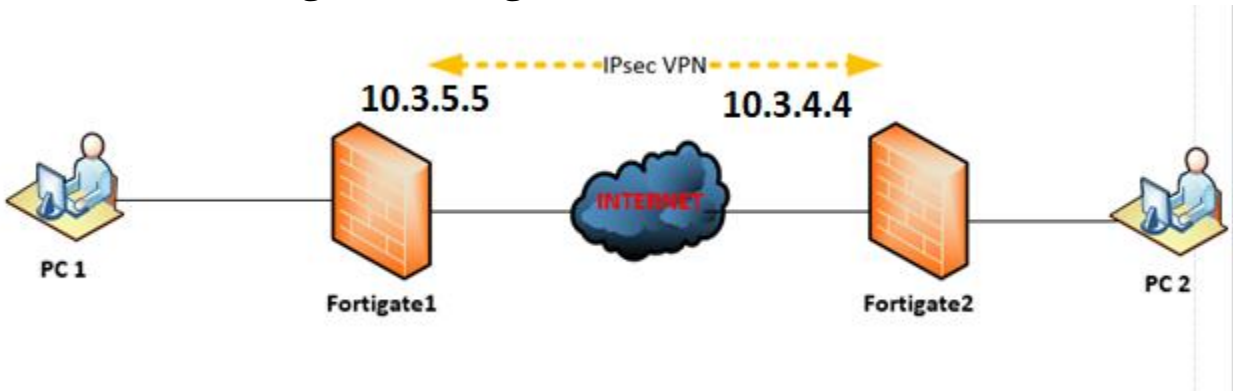
(Tuy nhiên trên version ảo chưa test được, có thể do chưa support)

Vào policy bật deep-inspection

Import CA cho user theo link này

<https://cookbook.fortinet.com/preventing-certificate-warnings/>

## 11. VPN IPsec giữa 2 Fortigate



Kết nối VPN IPsec giữa 2 fw, điều kiện giữa 2 WAN cần ping nhau ok đã  
Mục đích: tăng bảo mật trên đường truyền giữa 2 fw.

### Bước 1: trên Fortigate1

The screenshot shows the FortiGate VPN Creation Wizard interface. The left sidebar contains the navigation menu with 'VPN' selected and 'IPsec Wizard' highlighted. The main content area shows the 'VPN Creation Wizard' with three steps: 1. VPN Setup (active), 2. Authentication, and 3. Policy & Routing. The configuration options are as follows:

Name	FW1-to-FW2
Template Type	Site to Site   Remote Access   Custom
Remote Device Type	FortiGate   Cisco
NAT Configuration	No NAT between sites   This site is behind NAT   The remote site is behind NAT

VPN Creation Wizard

VPN Setup
  2 Authentication
  3 Policy & Routing

**Remote Device**
 IP Address
  Dynamic DNS

IP Address:

Outgoing Interface:

Detected via routing lookup

Authentication Method:  Pre-shared Key
  Signature

Pre-shared Key:

VPN Creation Wizard

VPN Setup
  Authentication
  3 Policy & Routing

Local Interface:

Local Subnets:

Remote Subnets:

Bước 2: Trên fortigate2 làm tương tự; lưu ý chỗ remote IP

**Kết quả**

- Vào **Monitor >> IPsec Monitor**

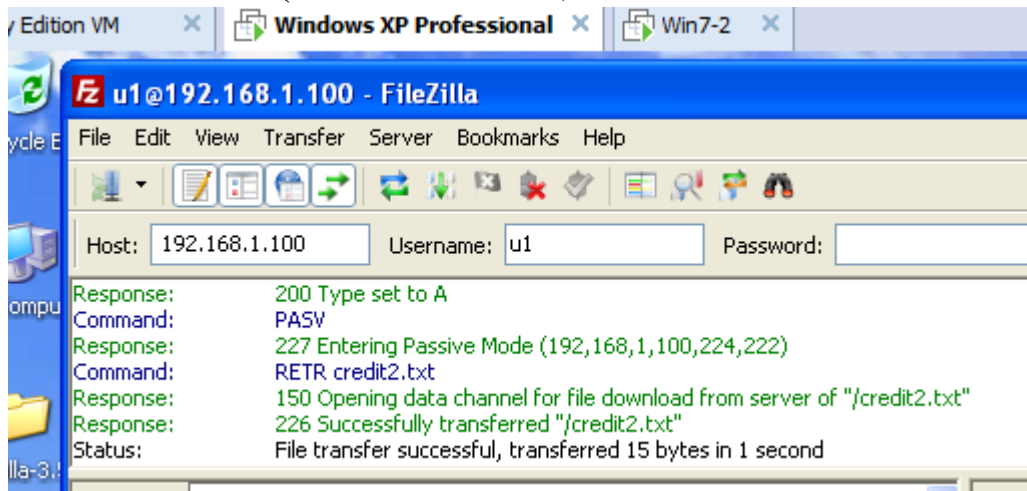
Bring up nó lên, up OK là được

Name	Type	Remote Gateway	User Name	Status
FW2-to-FW1	Site to Site - FortiGate	10.3.4.4		<input checked="" type="button" value="Up"/>

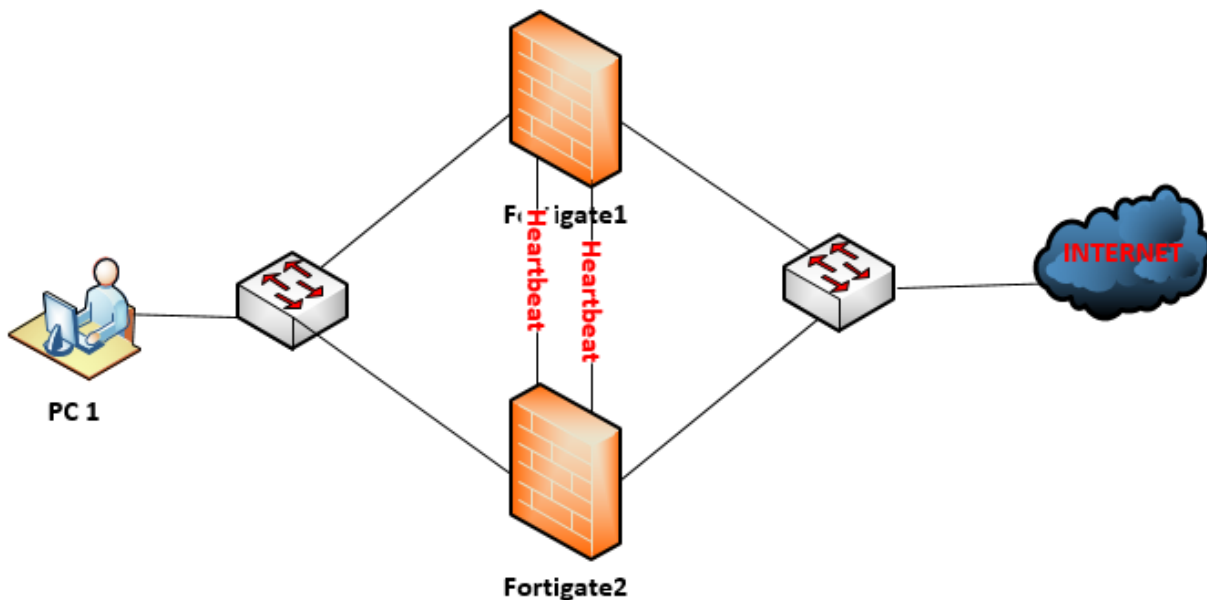
- Check ping giữa 2 LAN với nhau OK  
Check traffic đi qua Tunnel: có dung lượng

is	Incoming Data	Outgoing Data
	3.34 kB	1.90 kB

- Trên PC1, Bật FTP Filezilla lên download từ PC2 chỉ cần gõ LAN IP của Server là ok (do đã nối 2 LAN)



## 12. Hai tường lửa dự phòng (cơ chế Virtual MAC như VRRP)



Các bước:

Vào **System**>> **HA**, chọn Active/Passive, và điền như hình

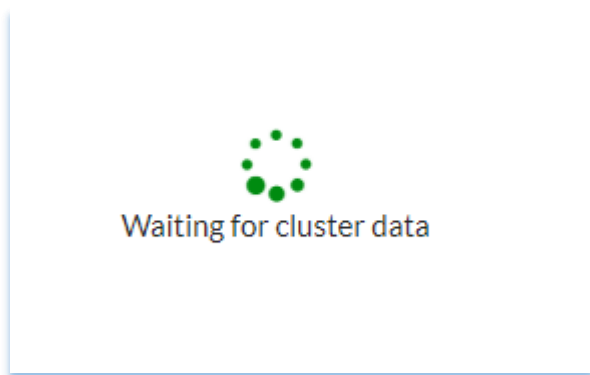
### Bên master:

The screenshot shows the configuration for High Availability (HA) on the master node. The 'High Availability' section is set to 'Active-Passive' mode with a 'Device priority' of 200. The 'Cluster Settings' section shows a group name of 'TESTLAB' and a password of 'minhhai123'. Under 'Monitor interfaces', 'WAN (port1)' and 'LAN (port2)' are selected. Under 'Heartbeat interfaces', 'port3' and 'port4' are selected. The 'Heartbeat Interface Priority' section shows sliders for 'port3' and 'port4' both set to 50. Red annotations highlight these settings: 'Bên master điền cao hơn 128' points to the priority value 200; 'minhhai123' points to the password; 'Port này để test link failure' points to the monitored interfaces; '02 Port nối giữa 2 FW' points to the heartbeat interfaces; and 'Để như này' points to the priority sliders.

### Bên Slave:

Điền giống như bên Master; chỉ khác chỗ priority để nguyên 128

Sau đó sẽ hiện như sau:





Sẽ ko truy cập trực tiếp vào web của Salve-Fortigate nữa

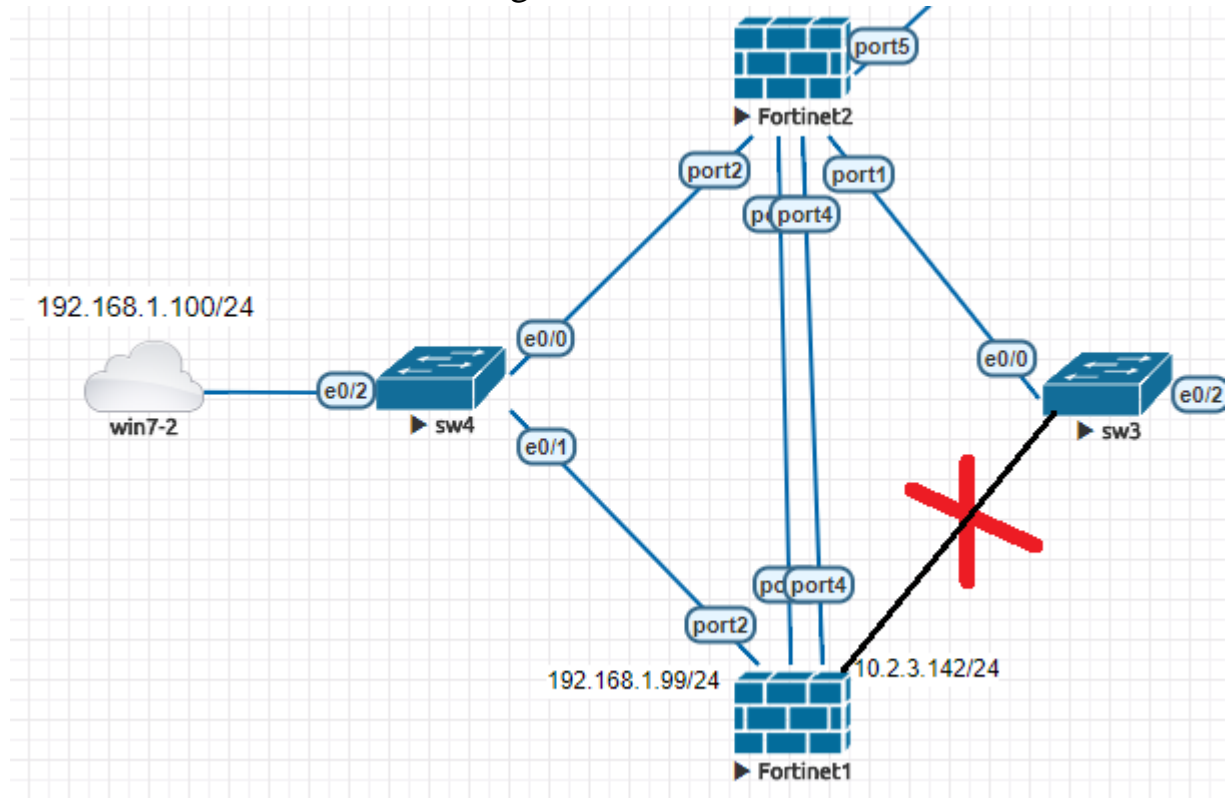
## Kết quả

- Thử down Master chính, vẫn ping OK

```
Command Prompt - ping google.com -t
Reply from 172.217.24.206: bytes=32 time=40ms TTL=53
Reply from 172.217.24.206: bytes=32 time=37ms TTL=53
Reply from 172.217.24.206: bytes=32 time=40ms TTL=53
Request timed out.
Reply from 172.217.24.206: bytes=32 time=38ms TTL=53
Reply from 172.217.24.206: bytes=32 time=37ms TTL=53
Reply from 172.217.24.206: bytes=32 time=40ms TTL=53
Reply from 172.217.24.206: bytes=32 time=40ms TTL=53
Reply from 172.217.24.206: bytes=32 time=41ms TTL=53
```

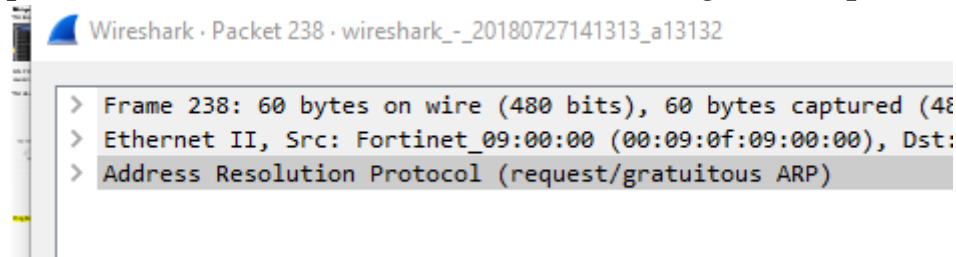
Khi FW ban đầu COME UP lại thì vẫn là slave chứ không quay lại master nữa (có dấu đỏ tức là đã từng down rồi up lại),

- Thử down link của master hướng lên internet



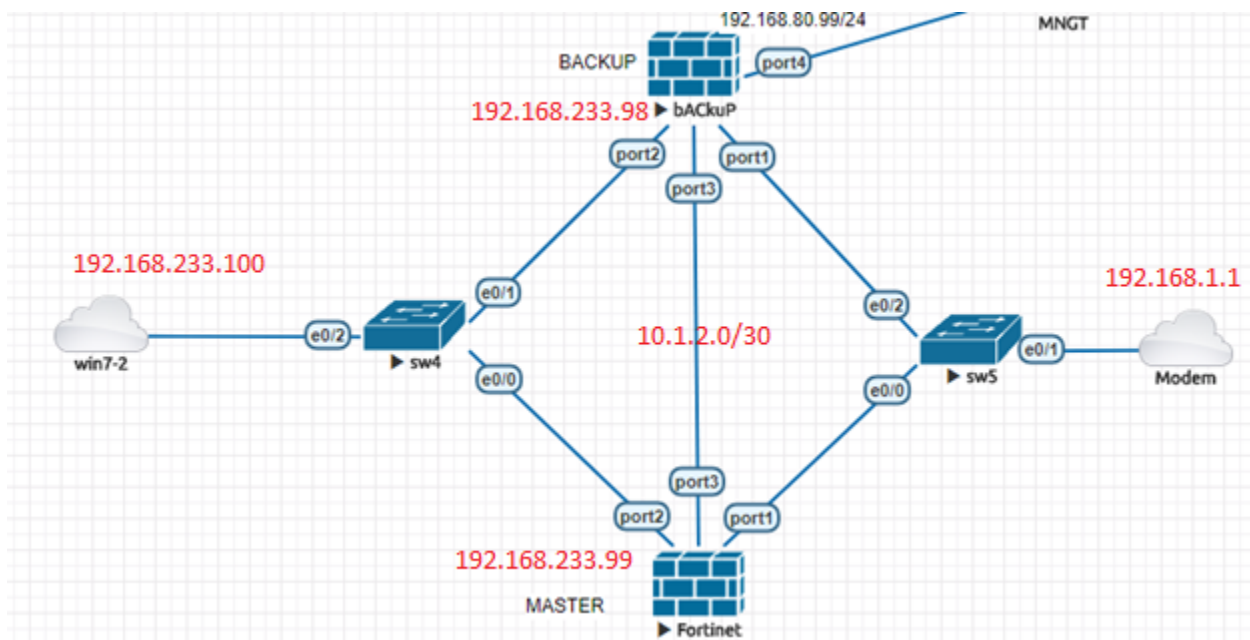
Ping failure-> có thể máy ảo nên ko hỗ trợ link failure

Khi master bị down thì node dự phòng gửi bản tin ARP gratuitous ra xung quanh để các đơn vị khác biết mà forwarding traffic qua nó



### 13. Cấu hình dự phòng wan internet

#### Cấu hình 2 FW/1 đường truyền




- Hướng chính: Win7-2 qua master ra internet
- Khi down port1 của master: thì traffic sẽ chạy qua port 3 sang Backup rồi ra mạng. Đặt static route trên Master: 0.0.0.0/0 qua port3 của Backup (với ad lớn hơn của route qua modem)
- Khi down cả con master thì Win7-2 sẽ chạy qua Backup (trên win7-2 add thêm 1 default route qua Backup với metric > metric của đg qua master)


## Trên Master:


Name	IP/Netmask
<u>port1</u>	192.168.1.99 255.255.255.0
<u>port2</u>	192.168.233.99 255.255.255.0
<u>port3 (giua 2 fw)</u>	10.1.2.1 255.255.255.252



Destination	Gateway	Interface
0.0.0.0/0	192.168.1.1	port1
0.0.0.0/0	10.1.2.2	port3



### Edit Policy


Name  to internet2



Incoming Interface  port2

Outgoing Interface  giua 2 fw (port3)

Source  all 

Destination  all 

Schedule  always

Service  ALL 

Action  ACCEPT  DENY  LEARN

### Firewall / Network Options

NAT

## Trên Backup

Name	IP/Netmask
<u>port1 (to internet)</u>	192.168.1.88 255.255.255.0
<u>port2</u>	192.168.233.98 255.255.255.0
<u>port3 (giua 2 fw)</u>	10.1.2.2 255.255.255.252

+ Create New   Edit   Clone   Delete

Destination	Gateway	
0.0.0.0/0	192.168.1.1	port1

### Edit Policy

Name **port3**

Incoming Interface **giua 2 fw (port3)**

Outgoing Interface **to internet (port1)**

Source **all**

Destination **all**

Schedule **always**

Service **ALL**

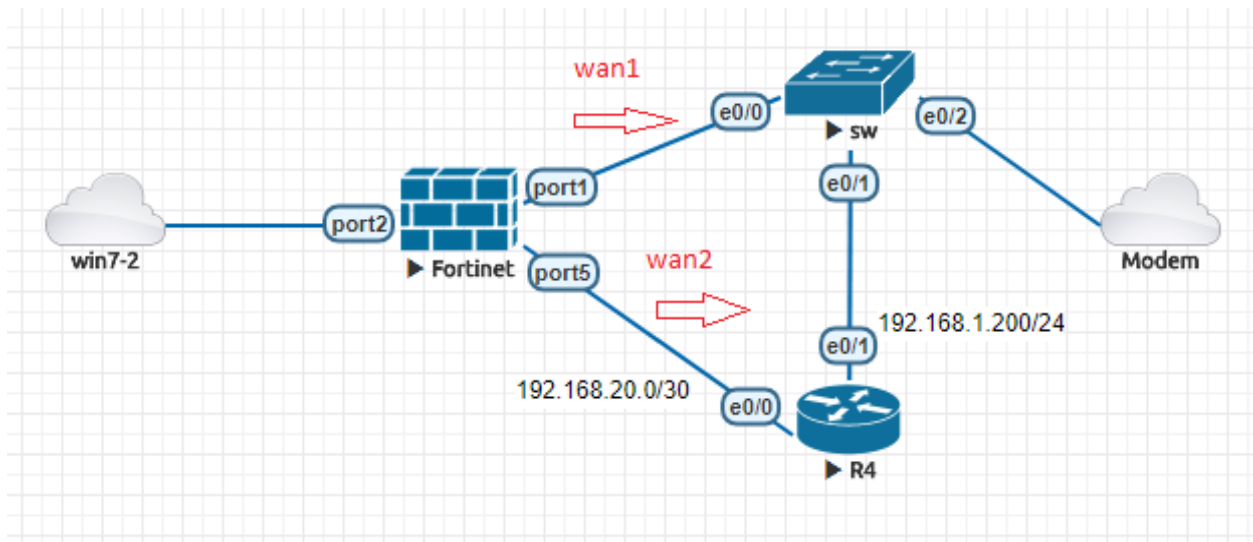
Action **ACCEPT**   DENY   LEARN

### Firewall / Network Options

NAT

IP Pool Configuration **Use Outgoing Interface Address**   Use Dynamic IP Pool

**Cấu hình 2 wan dự phòng internet**



Mục đích: traffic đi trên cả 2 đường wan1/2 (75%-25%)

Khi đứt 1 trong 2 wan thì traffic chạy trên 1 đường còn lại. Hồi phục lại thì lại trở về ban đầu (75-25)

Cấu hình Firewall

- Dashboard >
- Security Fabric >
- FortiView >
- Network** >
  - Interfaces
  - DNS
  - 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**

Name: sd-wan

Type: SD-WAN Interface

Interface State: ➤ Enable ➤ Disable

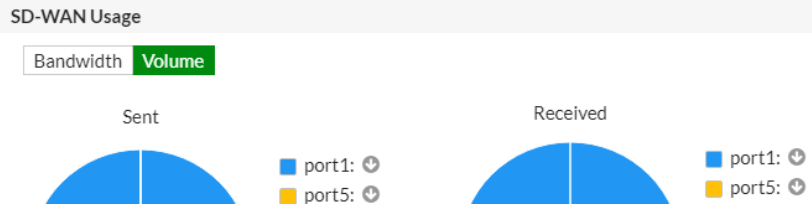
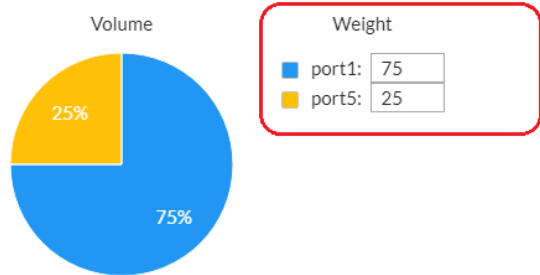
**SD-WAN**

+ Create New ✎ Edit 🗑 Delete

Seq.#	Interface	Status	Gateway
1	port1	✔	0.0.0.0
2	port5	✔	0.0.0.0

**Load Balancing Algorithm**

Volume
Sessions
Spillover
Source-Destination IP
Source IP



FortiGate VM64-KVM Master

- Dashboard
- Security Fabric
- FortiView
- Network
  - Interfaces
  - DNS
  - SD-WAN
  - SD-WAN Status Check**
  - SD-WAN Rules
  - Static Routes
  - Policy Routes
  - RIP
  - OSPF
  - BGP

### Edit SD-WAN Status Check

Name: pinggoogle

Protocol: **Ping** HTTP

Server: 8.8.8.8

#### Link Status

Timeout: 1 Second(s)

Failures before inactive: 5

Restore link after: 5

#### Actions when Inactive

Update static route:

+ Create New Edit Clone Delete

Destination	Gateway	
0.0.0/0	192.168.1.1	port1
0.0.0/0	192.168.20.4	port5

Kết quả:

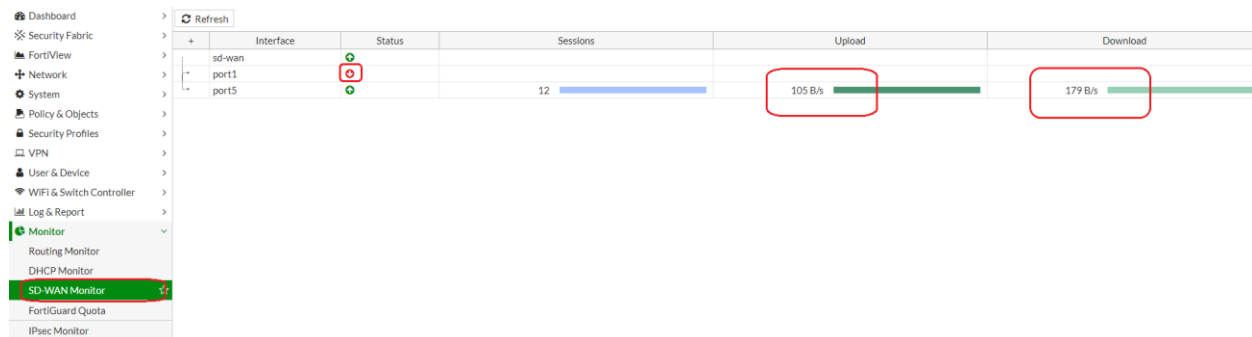
Từ Win7-2 ping google.com bình thường

```
C:\Users\ANSU>ping google.com -t
Pinging google.com [216.58.203.14] with 32 bytes of data:
Reply from 216.58.203.14: bytes=32 time=60ms TTL=54
Reply from 216.58.203.14: bytes=32 time=59ms TTL=54
Reply from 216.58.203.14: bytes=32 time=60ms TTL=54
Reply from 216.58.203.14: bytes=32 time=60ms TTL=54
```

Khi tắt đường wan1 thì sẽ bị mất dịch vụ 1 lúc

```
Reply from 192.168.233.99: Destination net unreachable.  
Reply from 192.168.233.99: Destination net unreachable.  
Reply from 192.168.233.99: Destination net unreachable.  
Reply from 192.168.233.99: Destination net unreachable.  
Reply from 192.168.233.99: Destination net unreachable.  
Reply from 216.58.203.14: bytes=32 time=60ms TTL=53  
Reply from 216.58.203.14: bytes=32 time=61ms TTL=53  
Reply from 216.58.203.14: bytes=32 time=62ms TTL=53  
Reply from 216.58.203.14: bytes=32 time=60ms TTL=53  
Reply from 216.58.203.14: bytes=32 time=60ms TTL=53  
Reply from 216.58.203.14: bytes=32 time=61ms TTL=53
```

Khi này tất cả traffic sẽ chạy qua wan2 (đường wan1 bị báo đỏ)



Mở lại wan1 thì 1 lúc sau tải lại chạy qua wan1 nhiều hơn so với wan2

Upload		Download	
88 B/s		188 B/s	
40 B/s		69 B/s	



Có phương pháp dự phòng internet khác là như link sau (dùng 2 static route, traffic chỉ chạy qua 1 wan)

<https://cookbook.fortinet.com/redundant-internet-basic-failover-56/>

## 14. **Cấu hình IPS sensor**

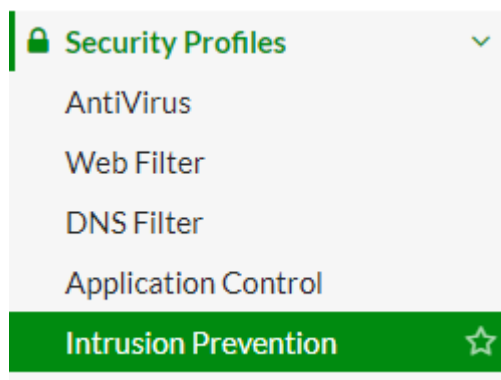
Mục đích: Scan traffic để phát hiện bất thường

Kết hợp DoS policy để bảo vệ các máy chủ đằng sau tường lửa

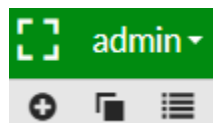
Ex1:

### **Cấu hình chặn file virus eicar**

Bước 1: tạo bộ lọc



Tạo mới, ấn dấu +



Đặt tên

-----

Edit IPS Sensor

Name

Comments  13/255

## Add signature


> IPS Signatures

>

+ Add Signatures    Delete    Edit IP Exemptions

Name	Exempt IPs
Eicar.Virus.Test.File	0

## Action là block

Action
 Block

## Apply vào policy đi internet

Sau đó thử vào máy tính download file eircar thì không down được; bỏ action block thì lại down được.


## 15. Giám sát log người dùng

- Vào 2 mục Log & Report hoặc Monitor hoặc FortiView (nhiều tính năng lưu log cần có disk, nhưng trên thiết bị ảo không có disk, chỉ có lưu memory nên chưa test được)

FortiView

Traffic From LAN/DMZ

Sources

Source	Source Device	Bytes (Sent/Received) ▾
192.168.1.100		6.33 kB 

## 16. Bóp băng thông

Enable shaping:

Advanced

Feature Visibility ☆

Certificates

Traffic Shaping +

Wireless Open Security +

Vào Policy&Objects > Traffic Shapers

Edit Traffic Shaper

Type Shared Per-IP

Name

Apply shaper Per policy All policies using this shaper

Traffic Priority

Max Bandwidth   Kbps

Guaranteed Bandwidth   Kbps

DSCP

OK
Cancel

Name	Type	Guaranteed Bandwidth
guarantee-100kbps	Shared	100 Kbps
high-priority	Shared	
limit_bw		
low-priority		
medium-priority		
shared-1M-pipe		

- Edit
- >\_ Edit in CLI**
- Clone
- Delete
- Clear Counters
- Show in FortiView

```
config firewall shaper traffic-shaper
edit "limit_bw"
set guaranteed-bandwidth 10
set maximum-bandwidth 20
set priority medium
set per-policy enable
next
```

Vào Policy&Objects > Traffic Shapping Policy

Tạo 2 cái policy:

- Cái 1: áp dụng cho riêng host 192.168.1.100
- Cái 2: để allow all traffic khác vẫn chạy bình thường

IPv4 (1 - 2)						
2	1	• limit_bw	• all	• WAN (port1)	limit_bw	limit_bw
1	2	• all	• all	• WAN (port1)	high-priority	high-priority

## Kết quả:

Vào website trên host 192.168.1.100, rồi vào check bw

Name	Type	Guaranteed Bandwidth	Max Band
guarantee-100kbps	Shared	100 Kbps	1048576 K
high-priority	Shared		1048576 K
limit_bw	Shared	10 Kbps	200 Kbps
low-priority	Shared		1048576 K
medium-priority	Shared		1048576 K
shared-1M-pipe	Shared		1024 Kbps

- Edit
- Edit in CLI
- Clone
- Delete
- Clear Counters
- Show in FortiView

Thấy đã theo dõi được bandwidth

Traffic Shaper: limit\_bw

Summary of limit\_bw

Bytes (Sent/Received)	3.59 kB
Bandwidth	496 bps
Sessions	8
Time Period	Realtime
FortiGate	FGVMEVCPWCNZFN77

Sources Destinations Applications Policies Sessions

Source	Source Device	Source Interface	Bytes (Sent/Received)	Sessions	Bandwidth
192.168.1.100		LAN (port2)	3.59 kB	8	496 bps

=====END=====

Xem các lớp học về firewall khác online (Checkpoint-Wireshark-Python)

<https://hainguyenit.edubit.vn>