HƯỚNG DẪN CẤU HÌNH VÀ QUẢN TRỊ

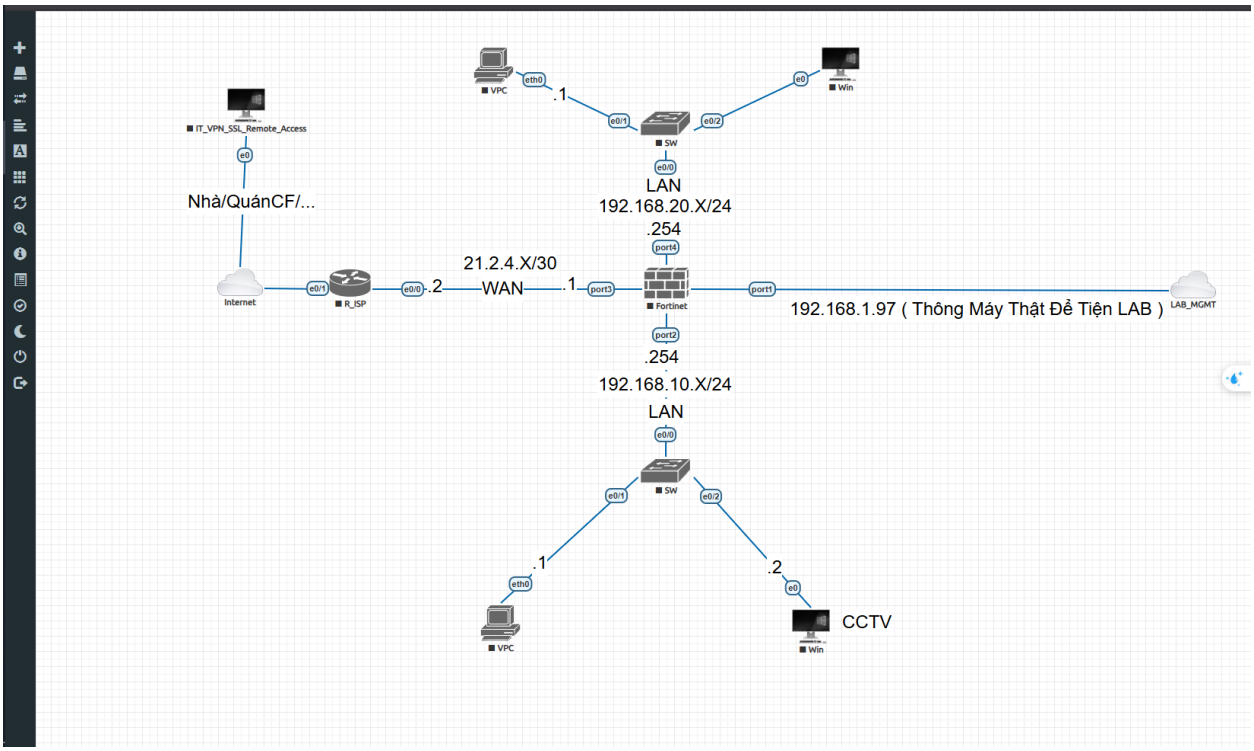
FORTIGATE 7.X

Dành cho sinh viên, kỹ sư mạng và người mới học firewall

Mục Lục

- 7. Quản lý, Logging và Xử lý sự cố
    - 7.1 Logging và Reporting
    - 7.2 Traffic Shaping
    - 7.3 Sao lưu và Khôi phục cấu hình
    - 7.4 Xử lý sự cố cơ bản (Basic Troubleshooting)
- 8. Phụ lục và Tham khảo
    - 8.1 Best Practices tổng hợp
    - 8.2 Các lỗi cấu hình thường gặp

Topology



1. Giới thiệu và truy cập thiết bị lần đầu (Initial Device Access)

Khi bắt đầu triển khai thiết bị FortiGate mới, chúng ta có hai phương thức truy cập chính: giao diện đồ họa (GUI) và cáp console (CLI). Việc lựa chọn phương thức phù hợp sẽ giúp quá trình cấu hình ban đầu thuận tiện và đảm bảo tính bảo mật.

1.1 Truy cập qua giao diện đồ họa (GUI)

- Mặc định, cổng **internal** (có thể ghi là *“internal”* hoặc *“port1”*) của FortiGate sử dụng địa chỉ IP **192.168.1.99**.

- Kết nối laptop với cổng này bằng cáp Ethernet.
- Thiết lập địa chỉ IP tĩnh cho laptop cùng dải mạng với FortiGate, ví dụ:
    - IP: 192.168.1.97
    - Subnet mask: 255.255.255.0
- Đăng nhập với:
    - **Username**: admin
    - **Password**: để trống

1.2 Truy cập qua cáp Console (CLI)

- Kết nối cáp console từ cổng console trên FortiGate đến cổng serial hoặc USB của laptop.
- Mở phần mềm terminal như **PuTTY** hoặc **SecureCRT**, thiết lập thông số:
    - Baud Rate: **9600**
    - Data Bits: **8**
    - Parity: **None**
    - Stop Bits: **1**
- Đăng nhập với:
    - Username: admin
    - Password: để trống

1.3 Gán địa chỉ IP tĩnh cho cổng FortiGate (CLI)

Sau khi đăng nhập CLI thành công, chúng ta thực hiện gán hoặc thay đổi địa chỉ IP tĩnh cho một cổng (ví dụ: port1) với các lệnh sau:

```
config system interface
edit port1
set mode static
set ip 192.168.1.97/24
set allowaccess ping https ssh http
next
end
```

Giải thích tham số:

- **set mode static**: cấu hình chế độ IP tĩnh cho interface
- **set ip**: gán địa chỉ IP và subnet mask
- **set allowaccess**: cho phép các phương thức truy cập quản trị (ping, https, ssh, http…)

Sau khi cấu hình, kiểm tra lại bằng lệnh:

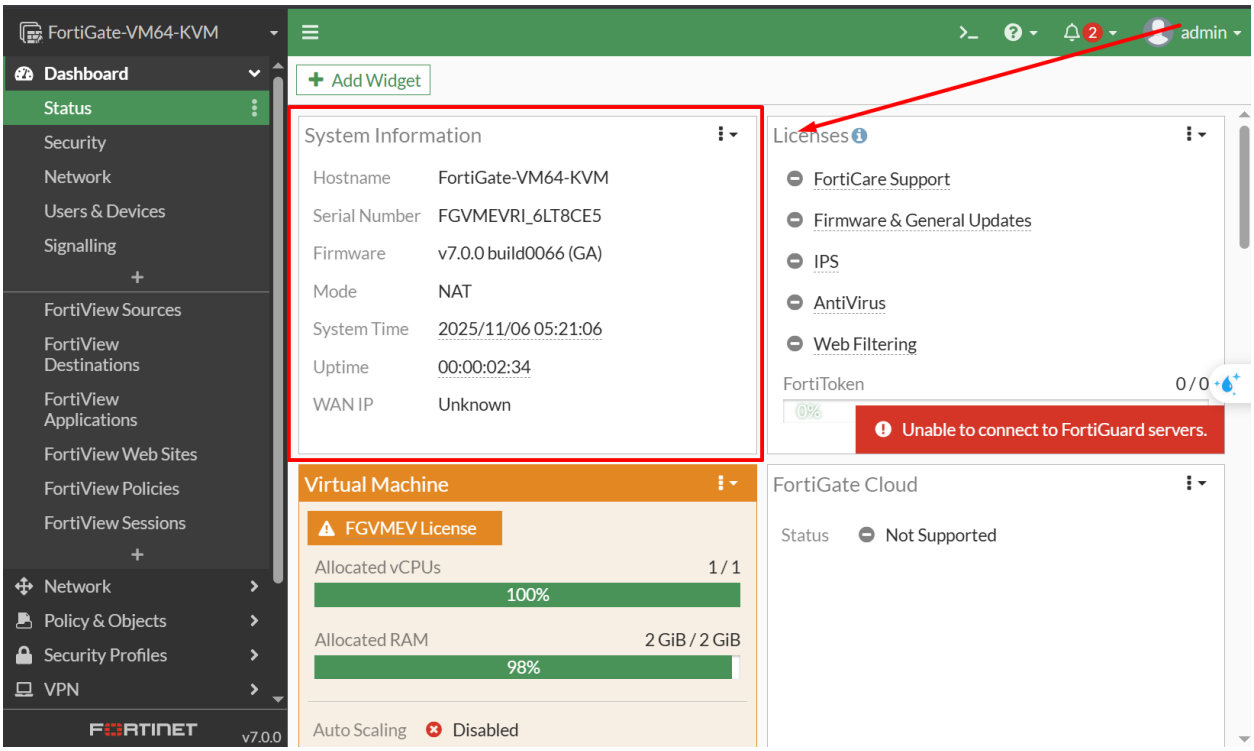
show system interface port1

Nếu cần truy cập qua trình duyệt, nhập địa chỉ IP mới vào thanh địa chỉ để đăng nhập GUI.

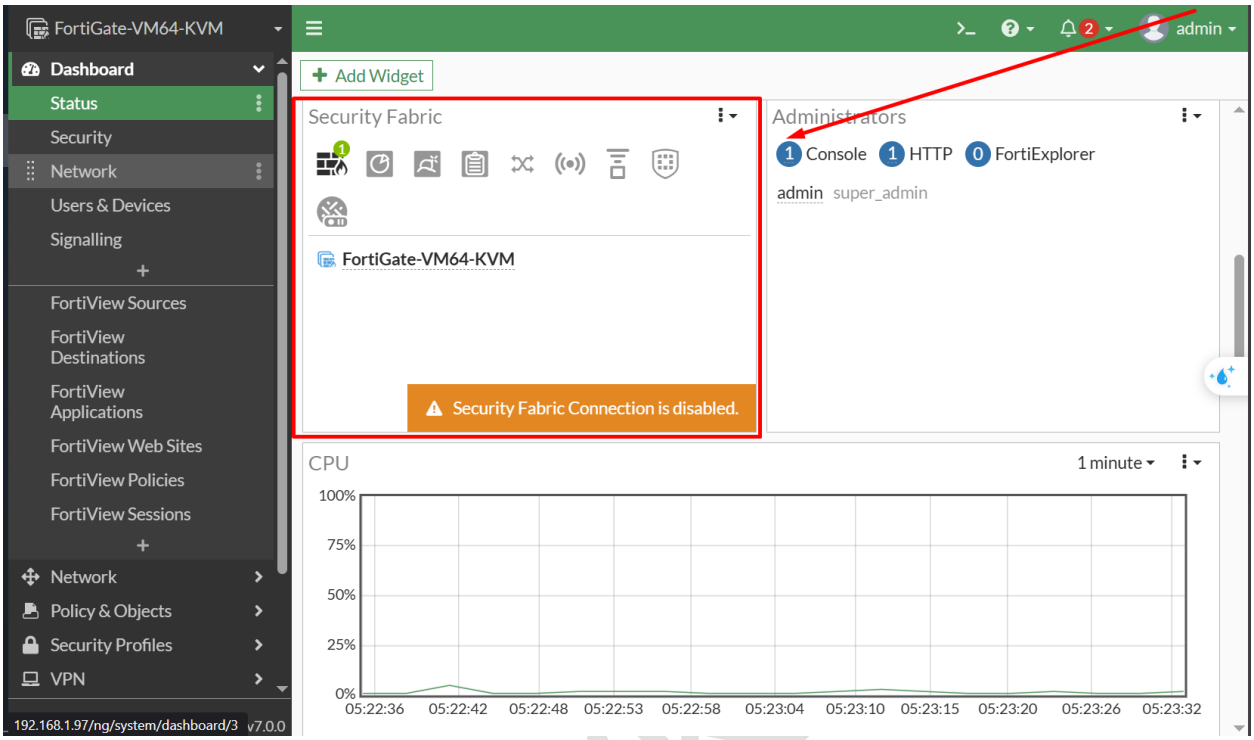
1.4 Tìm hiểu bảng điều khiển chính (Main Dashboard)

Sau khi đăng nhập, chúng ta tiếp cận bảng điều khiển trung tâm với các widget quan trọng:

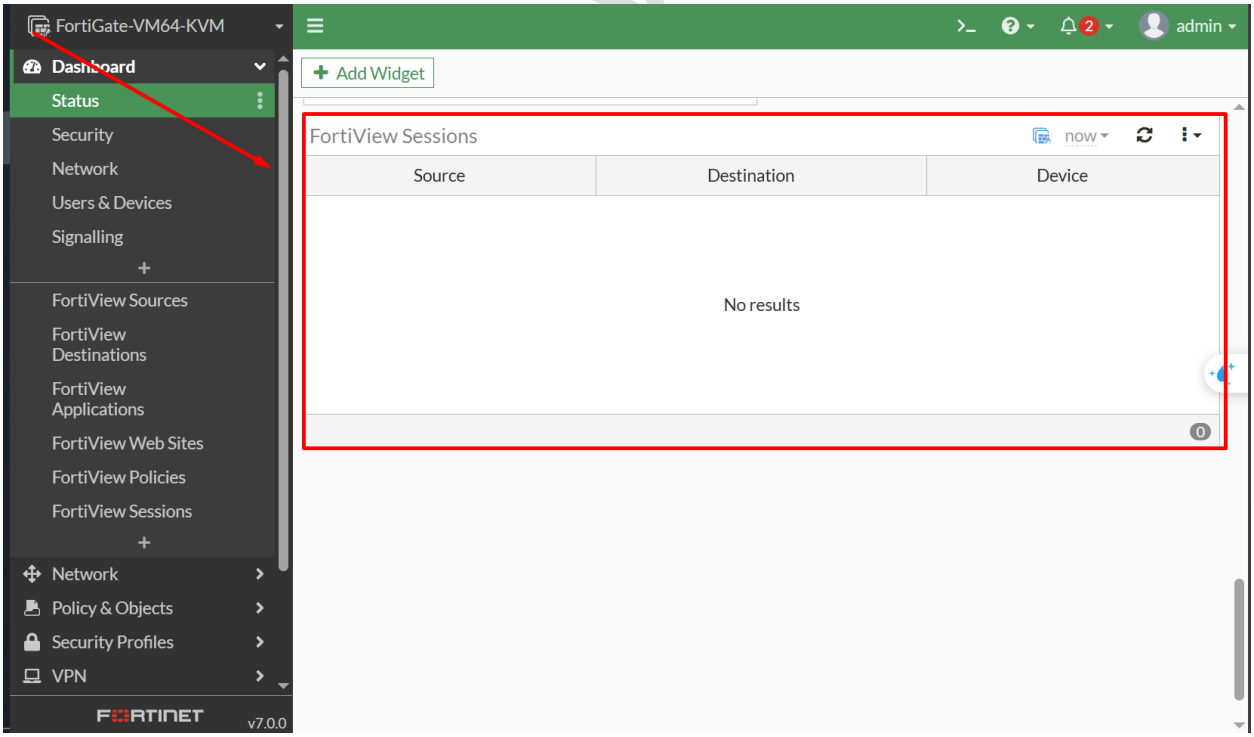
- **System Information**: Hiển thị model thiết bị, phiên bản FortiOS, thời gian hoạt động và trạng thái license.



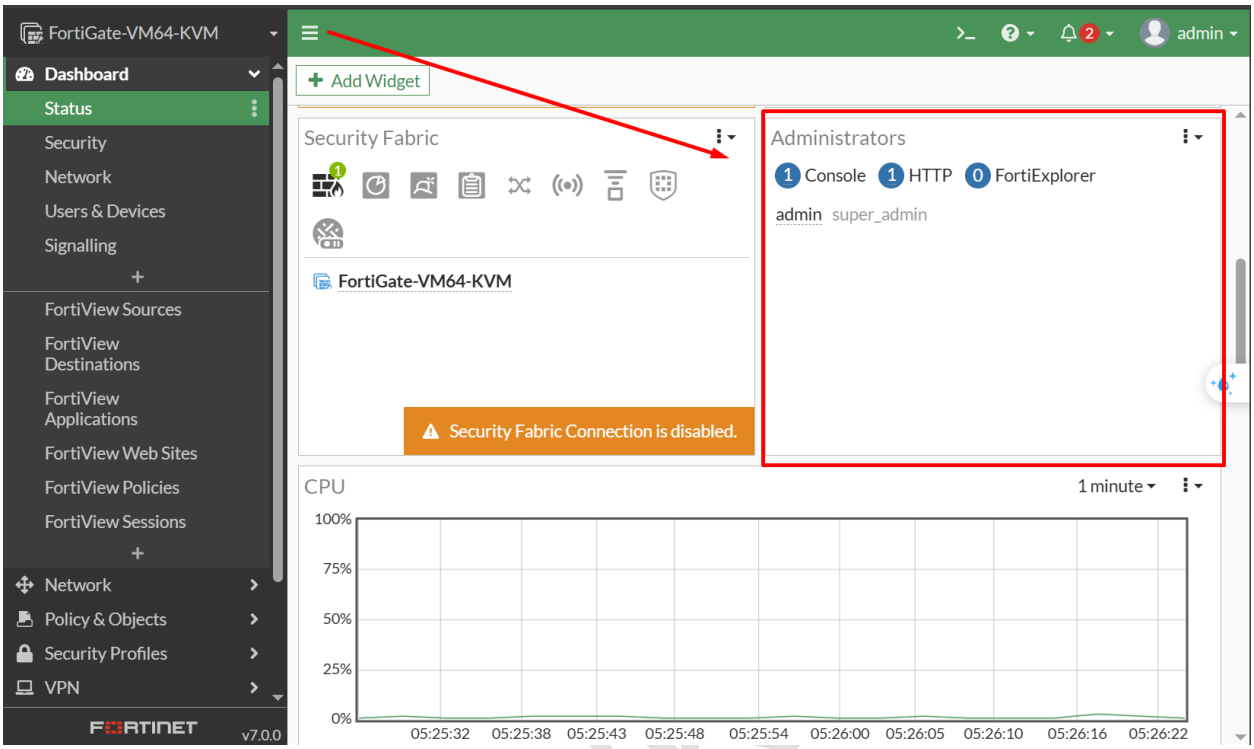
- **Security Fabric**: Hiển thị trạng thái kết nối với các thiết bị Fortinet khác.



- **FortiView**: Cung cấp biểu đồ thời gian thực về các phiên, nguồn, đích và ứng dụng qua tường lửa, hỗ trợ giám sát và xử lý sự cố.

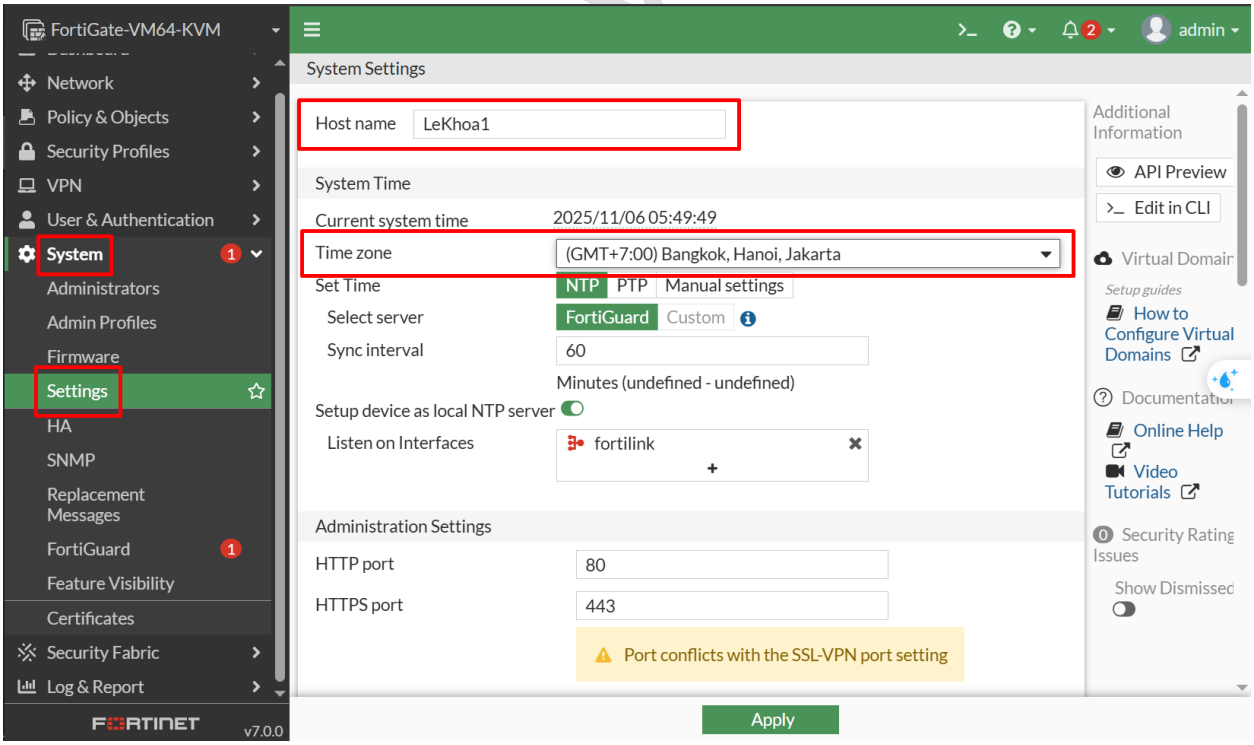


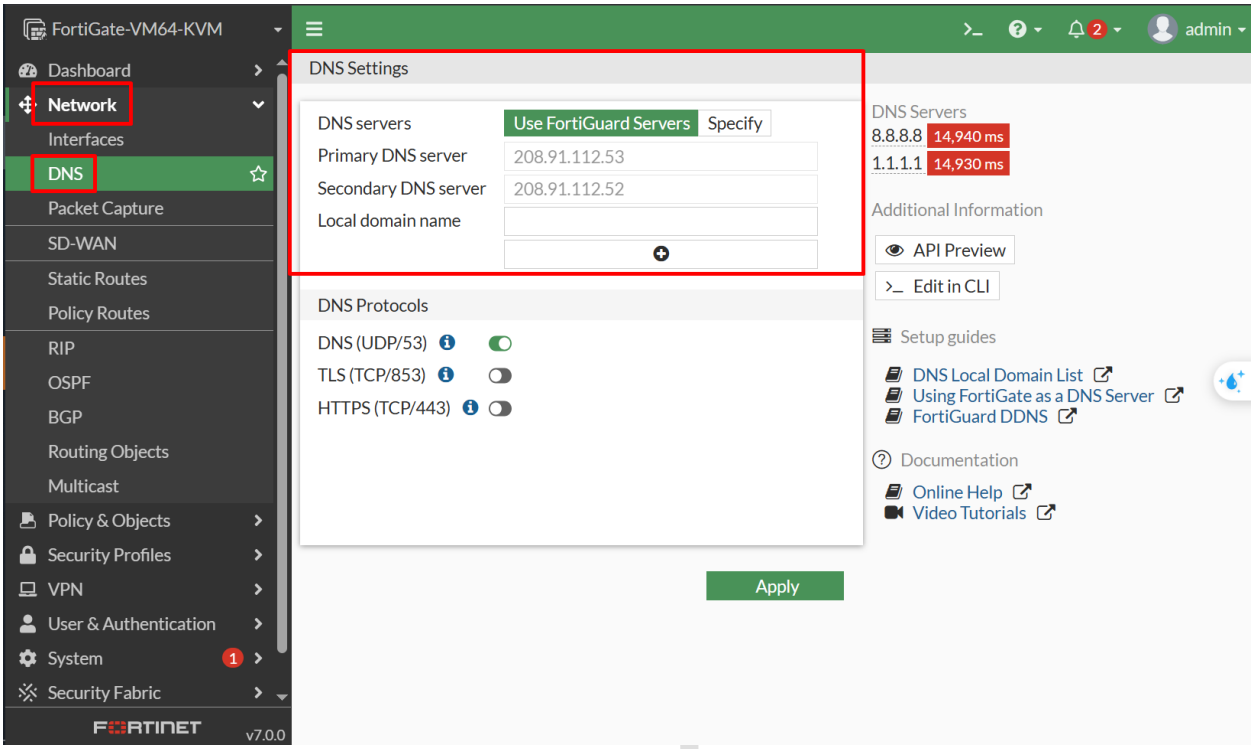
- **Administrators**: Hiển thị danh sách người dùng đăng nhập hệ thống.



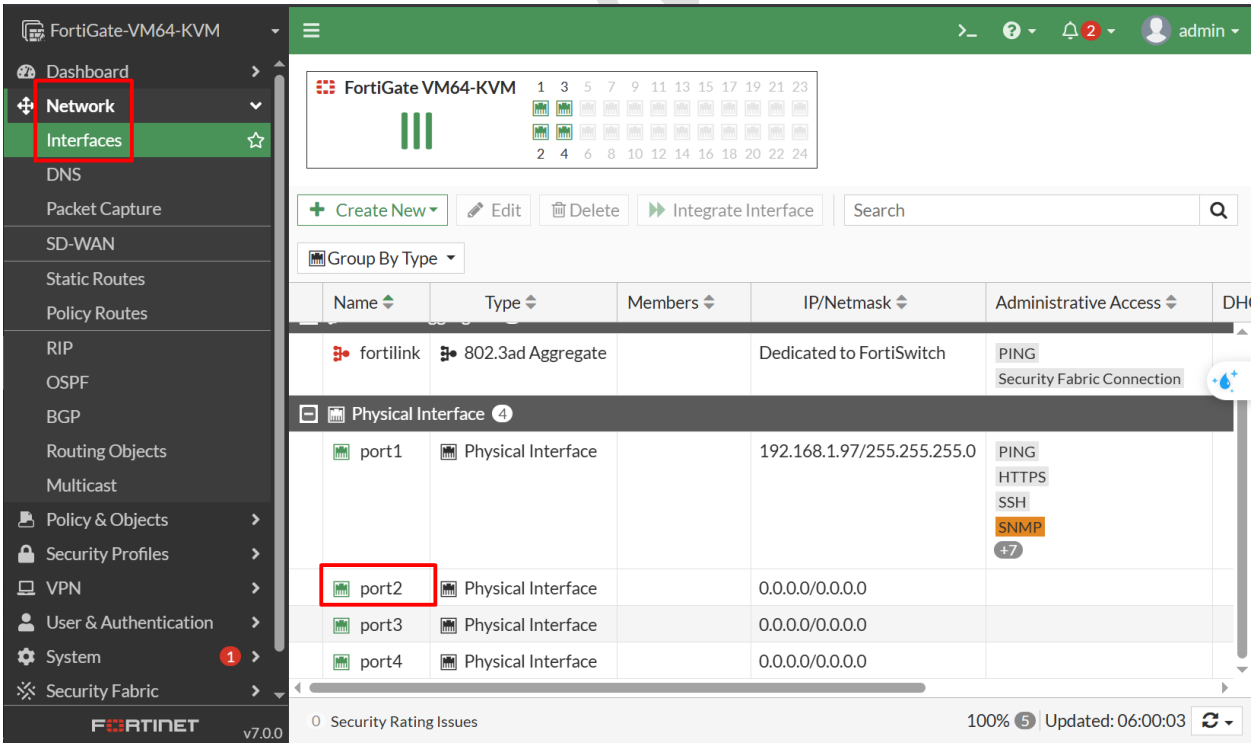
1.5 Cấu hình cơ bản ban đầu

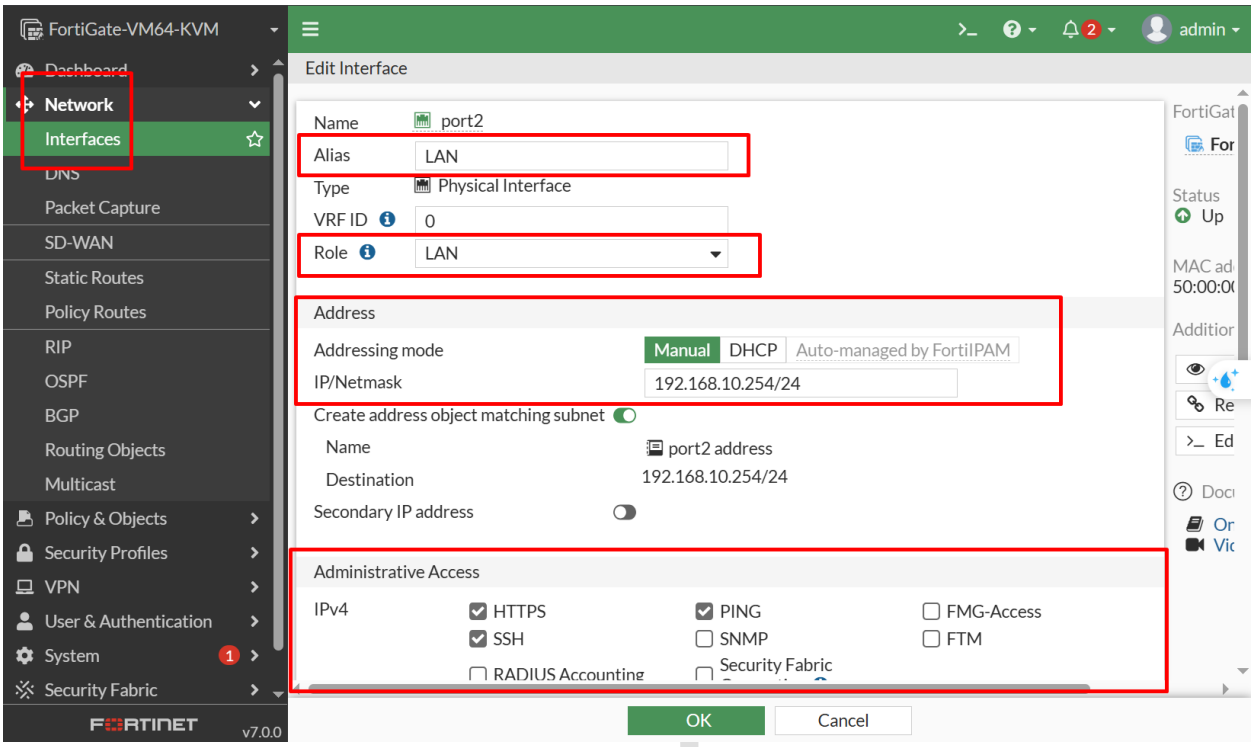
- Thiết lập hostname, DNS, timezone cho thiết bị.

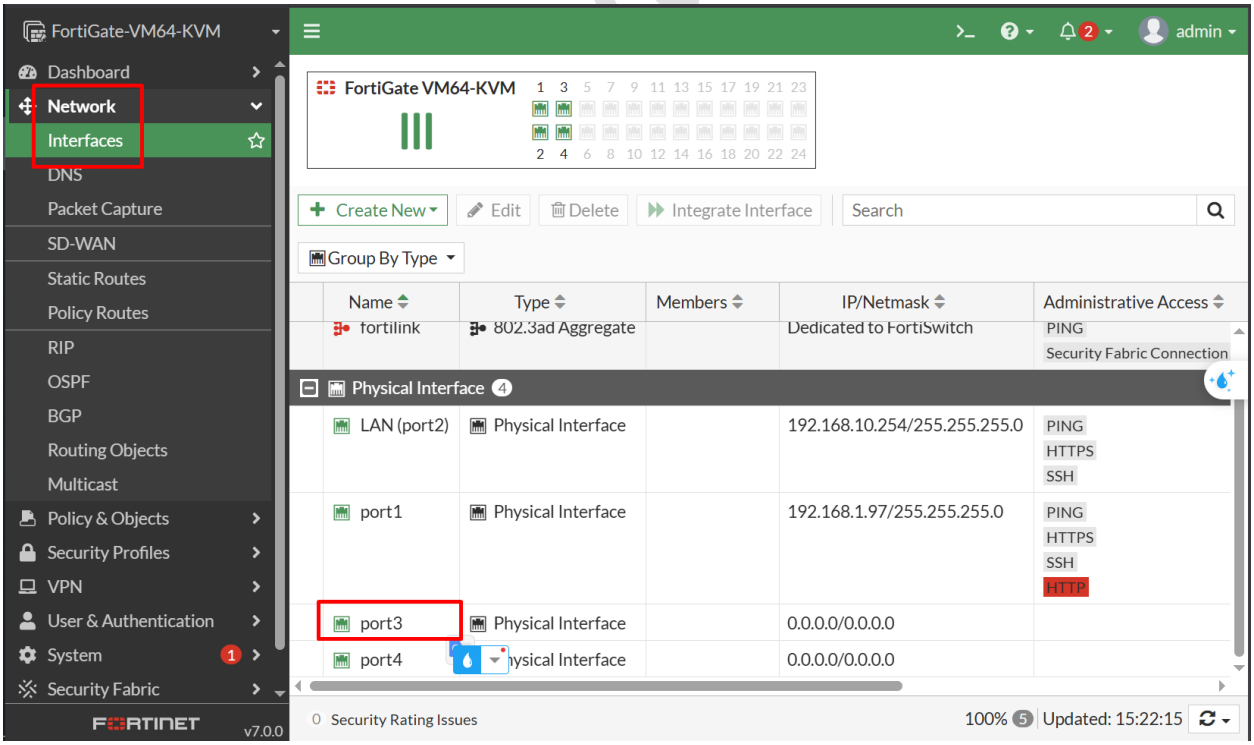


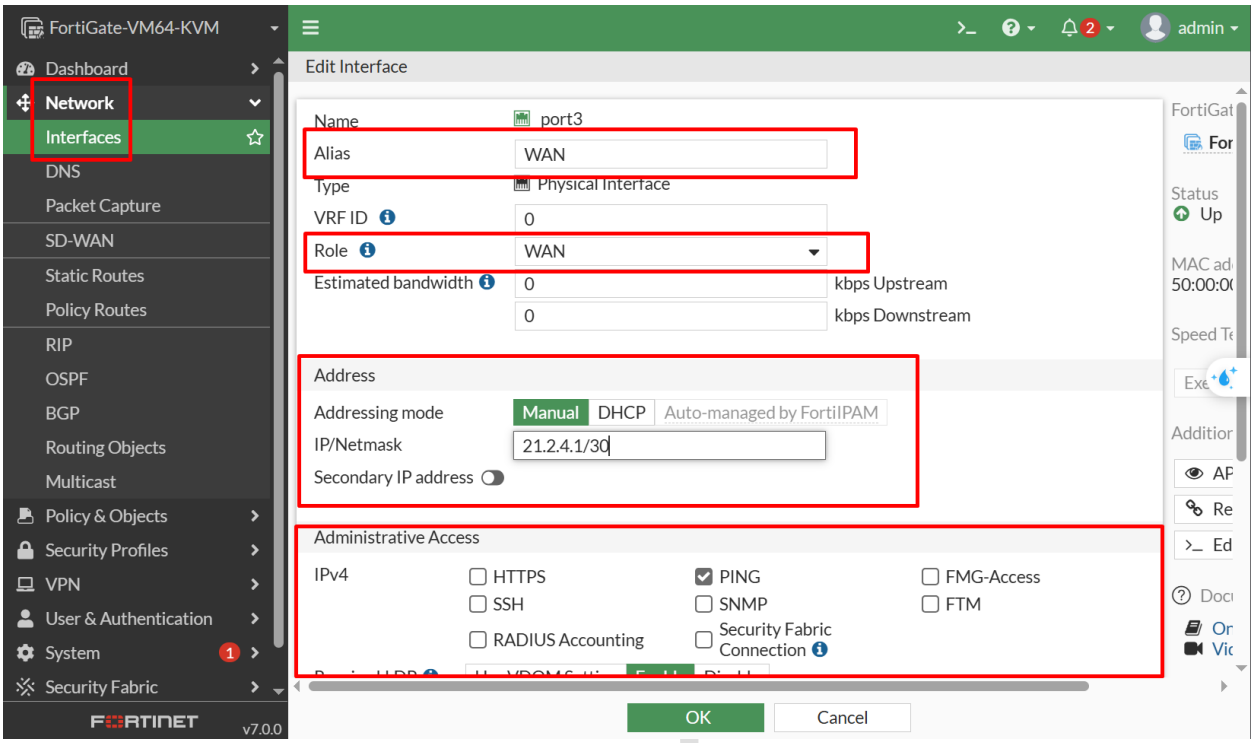


- Gán địa chỉ IP cho các cổng LAN/WAN.

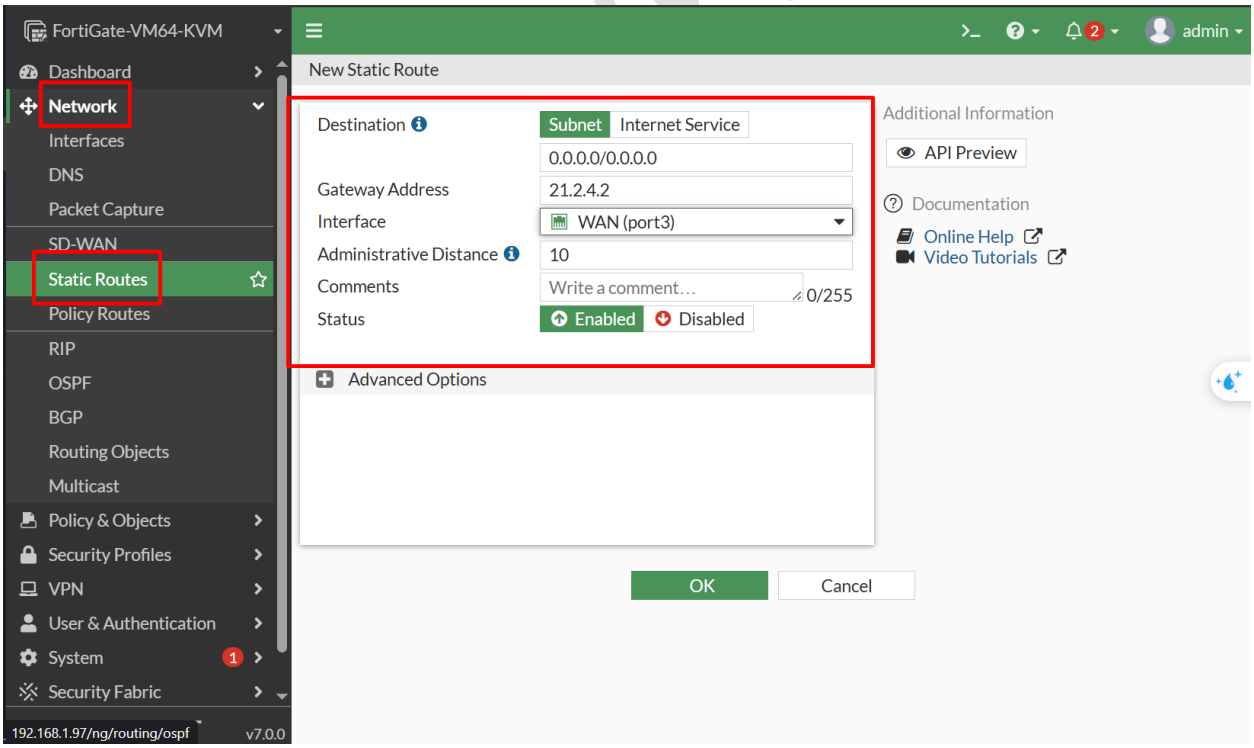


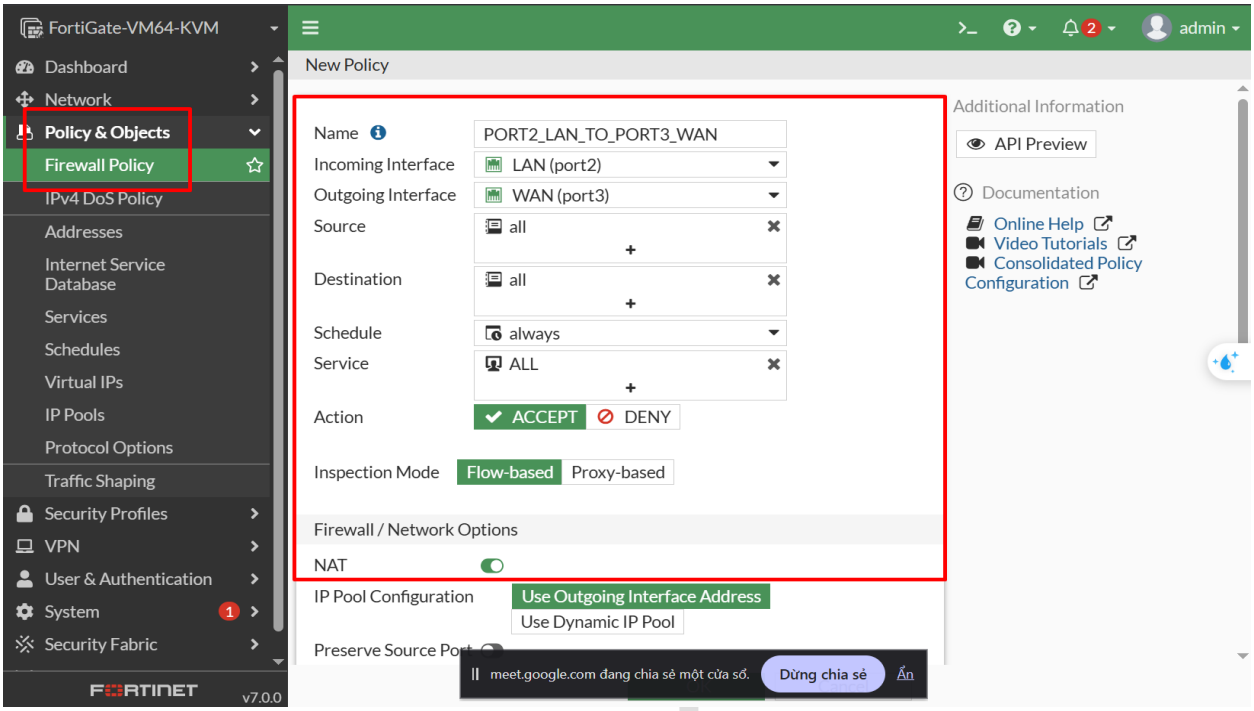

FortiGate-VM64-KVM
admin
Edit Interface
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Name port2
Alias LAN
Type Physical Interface
VRF ID 0
Role LAN
Address
Addressing mode Manual DHCP Auto-managed by FortiIPAM
IP/Netmask 192.168.10.254/24
Create address object matching subnet
Name port2 address
Destination 192.168.10.254/24
Secondary IP address
Administrative Access
IPv4
HTTPS
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric
OK
Cancel
FORTINET
v7.0.0


FortiGate-VM64-KVM
admin
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
FortiGate VM64-KVM
Create New
Edit
Delete
Integrate Interface
Search
Group By Type
Name
Type
Members
IP/Netmask
Administrative Access
fortilink
802.3ad Aggregate
Dedicated to FortiSwitch
PING
Security Fabric Connection
Physical Interface 4
LAN (port2)
Physical Interface
192.168.10.254/255.255.255.0
PING
HTTPS
SSH
port1
Physical Interface
192.168.1.97/255.255.255.0
PING
HTTPS
SSH
HTTP
port3
Physical Interface
0.0.0.0/0.0.0.0
port4
Physical Interface
0.0.0.0/0.0.0.0
Security Rating Issues
100%
Updated: 15:22:15
FORTINET
v7.0.0



- Kiểm tra kết nối Internet.





Sau khi hoàn thành các bước trên, thiết bị FortiGate đã sẵn sàng, bảo mật, cập nhật và chuẩn bị cho các cấu hình nâng cao.

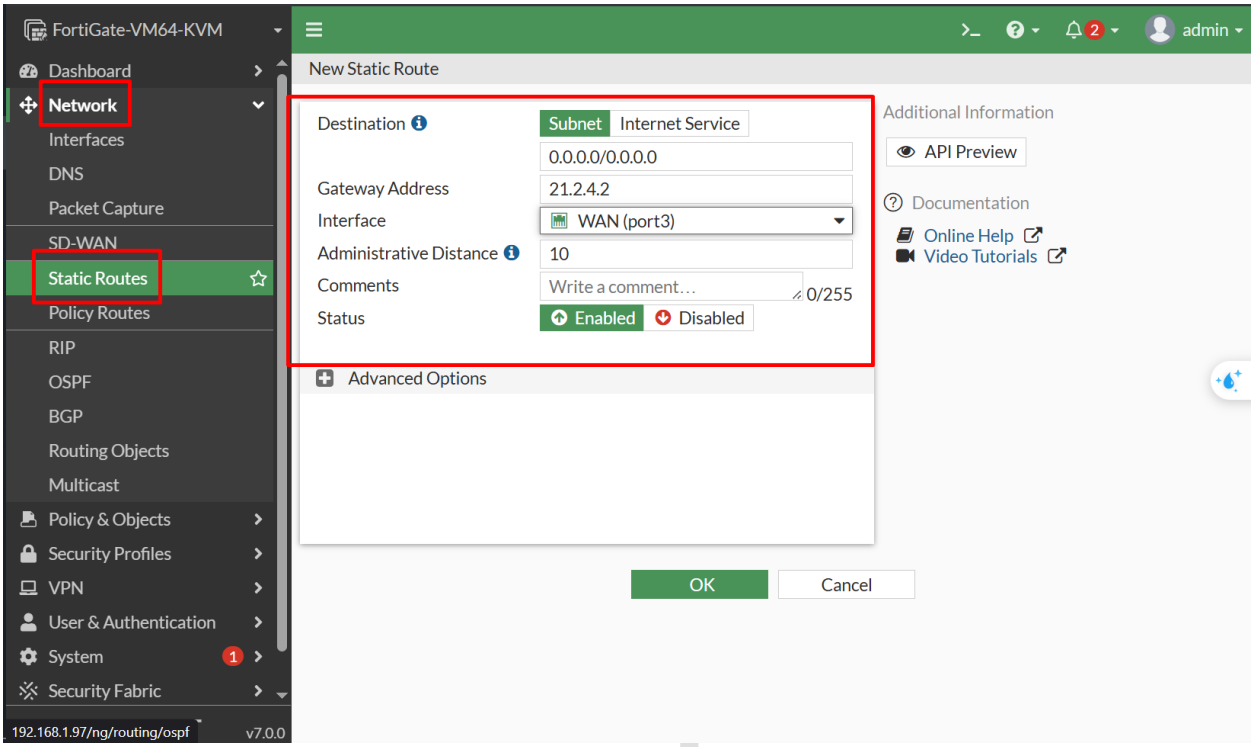
2. Cấu hình Mạng cơ bản (Network Basics)

Trong phần này, chúng ta thiết lập định tuyến (routing) để FortiGate chuyển tiếp lưu lượng đến Internet hoặc các mạng nội bộ khác. Có hai loại tuyến (route) cần lưu ý:

2.1 Default Route (Tuyến mặc định – 0.0.0.0/0)

- Tuyến mặc định giúp FortiGate gửi mọi lưu lượng không xác định đích ra Internet.
- Thông thường, tuyến này trỏ về gateway của ISP (modem hoặc router do nhà mạng cung cấp).
- Cấu hình ví dụ:
    - **Destination**: 0.0.0.0/0
    - **Gateway**: 21.2.4.2 *(địa chỉ gateway ISP)*
    - **Interface**: port3 *(cổng kết nối Internet)*

 Lưu ý: Nếu không cấu hình Default Route, các thiết bị trong mạng LAN sẽ không thể truy cập Internet. Default Route là tuyến định tuyến chuyển tiếp toàn bộ lưu lượng không xác định đích ra Internet qua gateway.



3. Chính sách tường lửa và Quản lý đối tượng (Firewall Policy & Object Management)

3.1 Cấu hình chính sách tường lửa đầu tiên (Configuring Your First Firewall Policy)

Trong phần này, chúng ta áp dụng kiến thức về FortiGate để cấu hình tình huống thực tế: cho phép toàn bộ người dùng mạng nội bộ (LAN) truy cập Internet (WAN) qua Firewall Policy. Các bước dưới đây sẽ hướng dẫn chi tiết quy trình cấu hình, đồng thời giải thích thuật ngữ tiếng Anh chuẩn Fortinet kèm diễn giải tiếng Việt ngắn gọn.

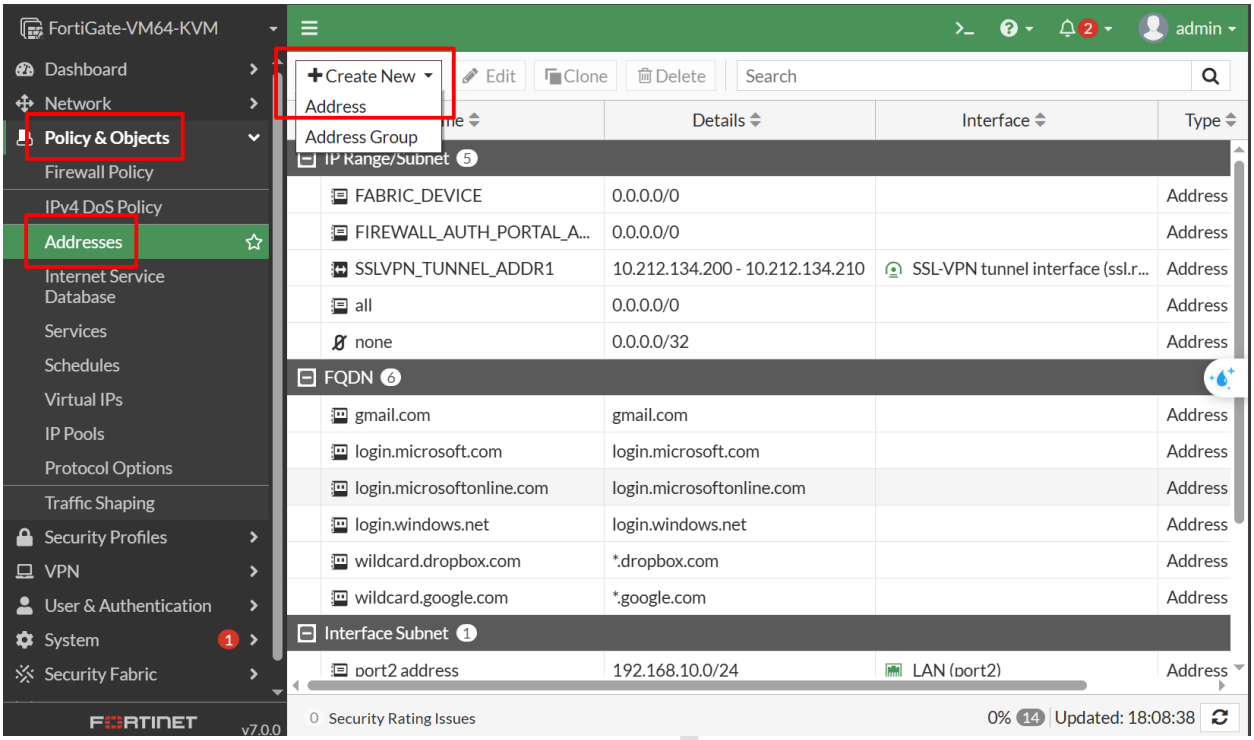
Tình huống thực tế

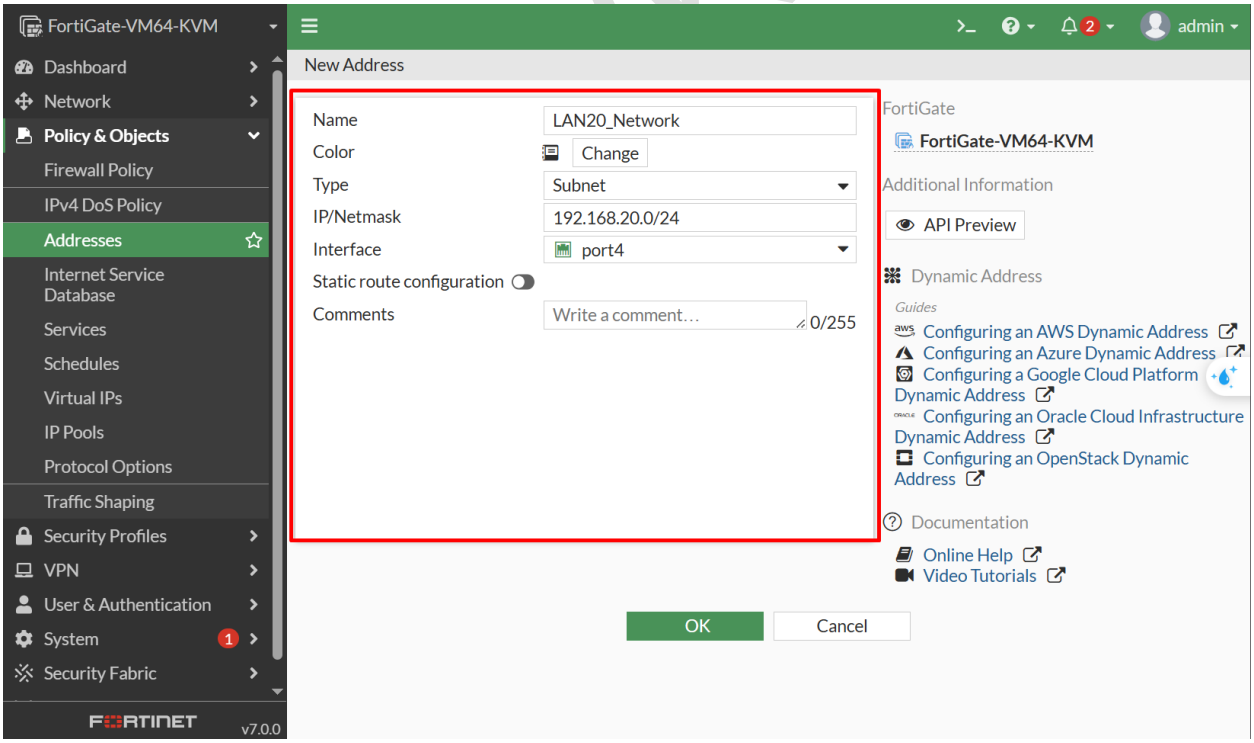
Yêu cầu: Cho phép tất cả người dùng thuộc mạng LAN truy cập Internet thông qua FortiGate Firewall Policy.

Các bước thực hiện

Bước 1: Tạo Address Object cho mạng LAN

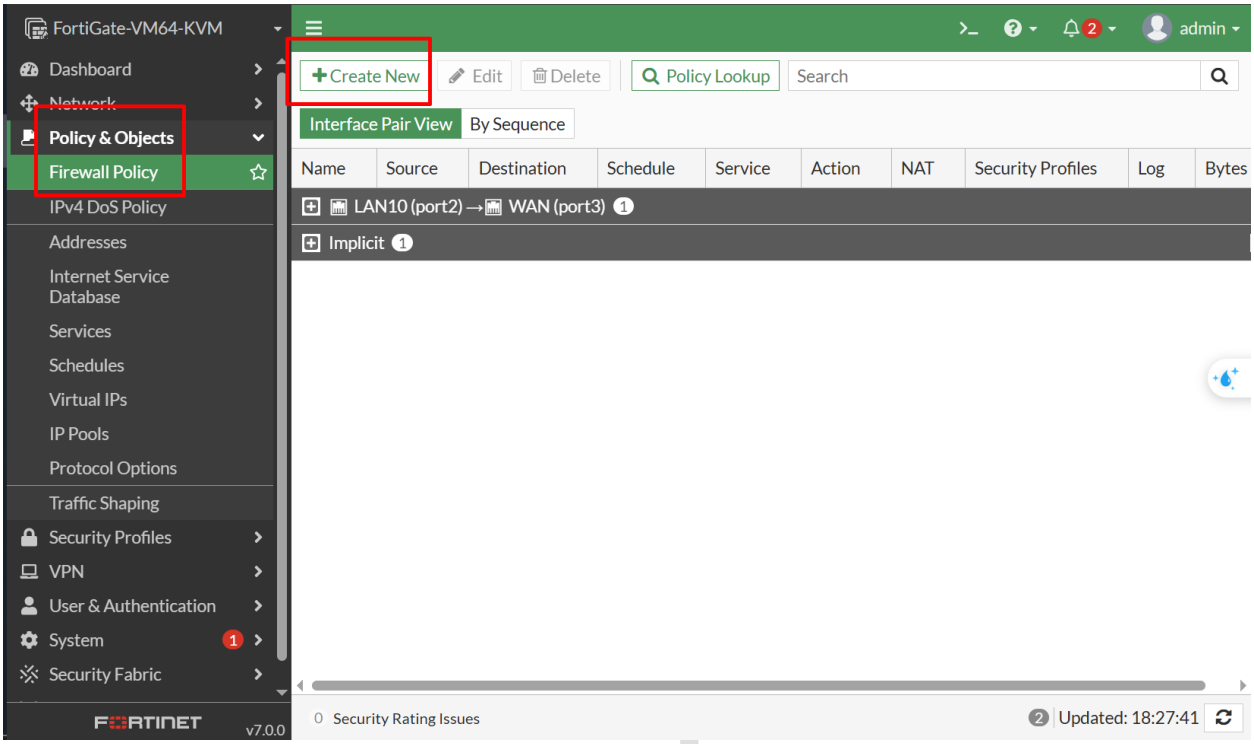
Truy cập **Policy & Objects > Addresses** để khai báo địa chỉ mạng nội bộ thông qua Address Object. Nếu chưa tồn tại đối tượng, thao tác như sau:

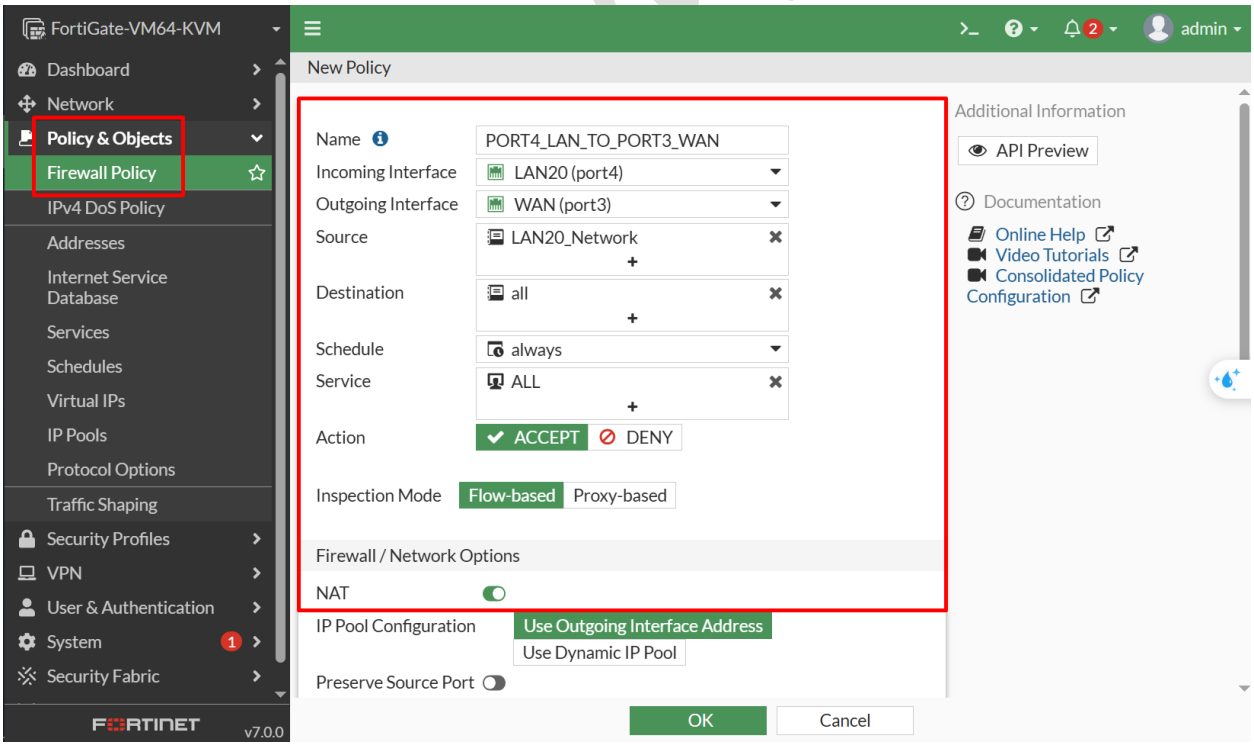




Bước 2: Tạo Firewall Policy

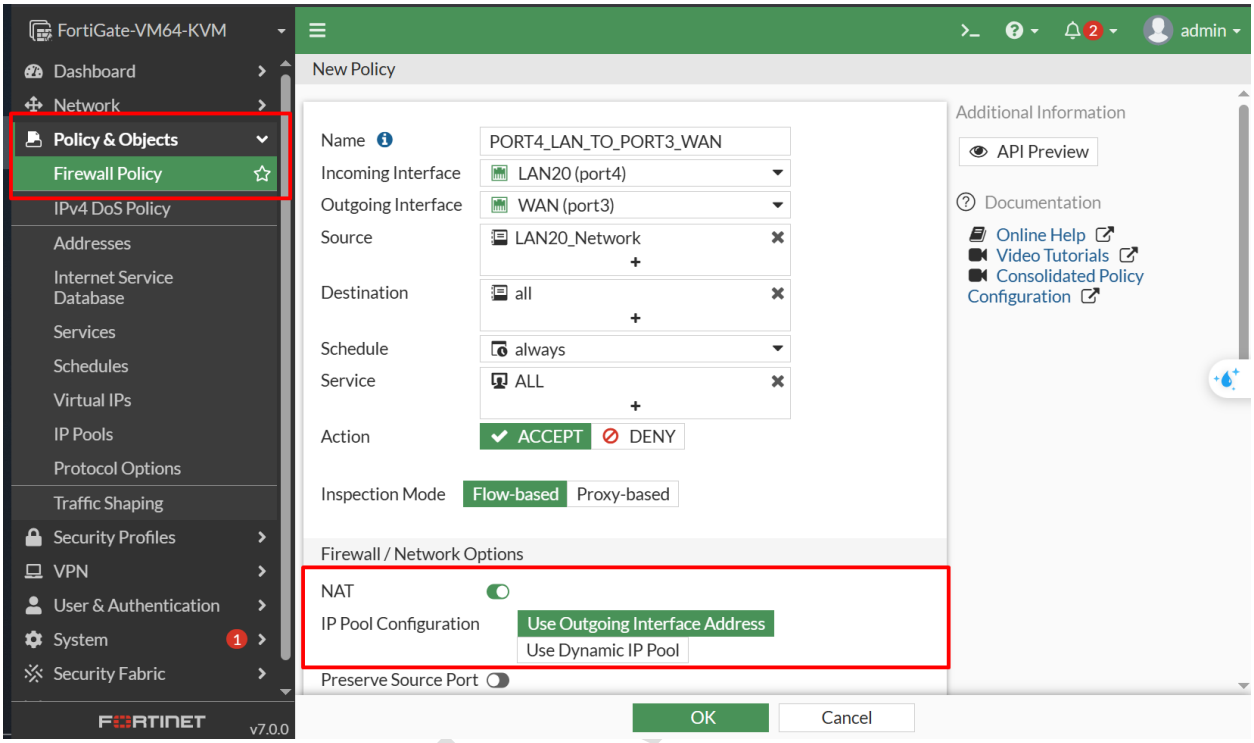
Truy cập **Policy & Objects > Firewall Policy** và nhấn **Create New** để tạo chính sách tường lửa. Cấu hình chi tiết như sau:


FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
FORTINET
v7.0.0
admin
Create New
Edit
Delete
Policy Lookup
Search
Interface Pair View
By Sequence
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
LAN10 (port2) → WAN (port3)
Implicit
0 Security Rating Issues
Updated: 18:27:41


FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
FORTINET
v7.0.0
admin
New Policy
Name
PORT4_LAN_TO_PORT3_WAN
Incoming Interface
LAN20 (port4)
Outgoing Interface
WAN (port3)
Source
LAN20_Network
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
OK
Cancel
Additional Information
API Preview
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration

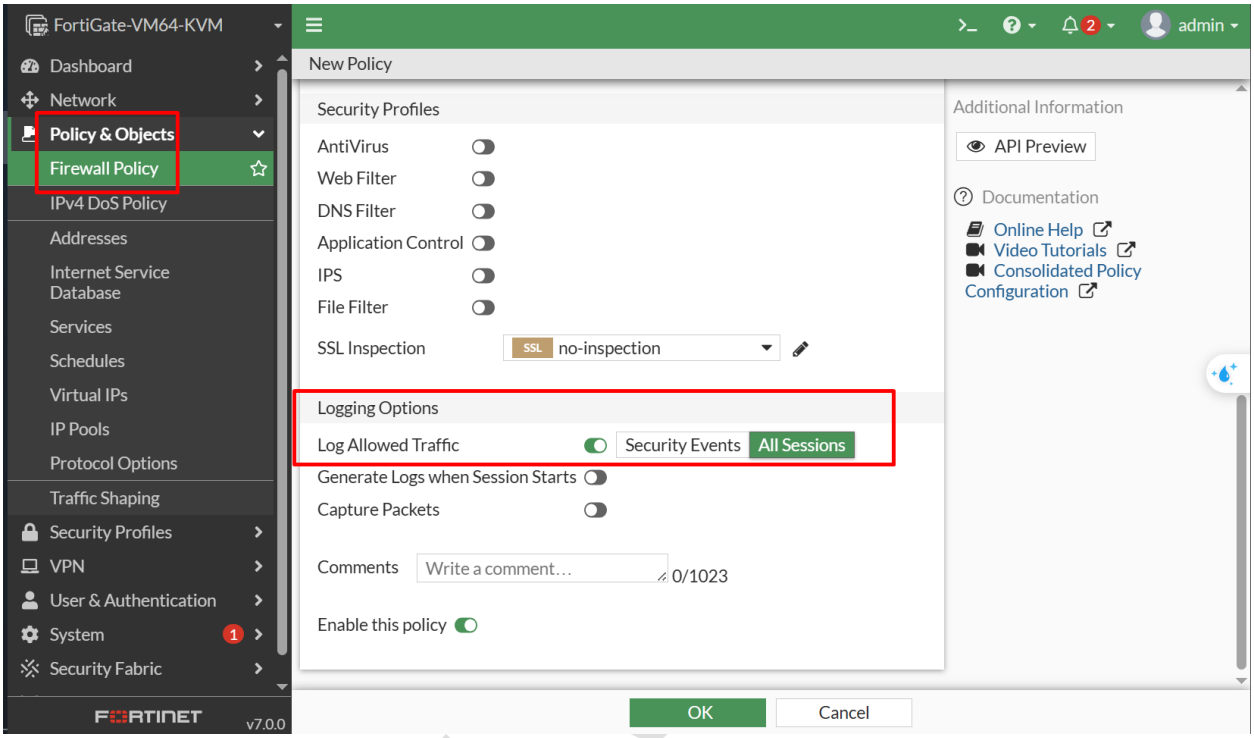
Bước 3: Bật NAT (Network Address Translation)

Kéo xuống phần **NAT** và bật **Use Outgoing Interface Address**. Thao tác này giúp các thiết bị trong LAN sử dụng địa chỉ IP công cộng của FortiGate khi truy cập Internet. NAT (Network Address Translation) là kỹ thuật chuyển đổi địa chỉ IP nguồn thành địa chỉ IP công cộng khi lưu lượng đi ra ngoài.



Bước 4: Bật Logging (Ghi nhật ký)

Tại mục **Logging Options**, bật **Log Allowed Traffic** và chọn **All Sessions**. Ghi nhật ký cho phép giám sát truy cập và hỗ trợ xử lý sự cố nhanh chóng. Sau khi hoàn tất, nhấn **OK** để lưu lại cấu hình chính sách tường lửa.

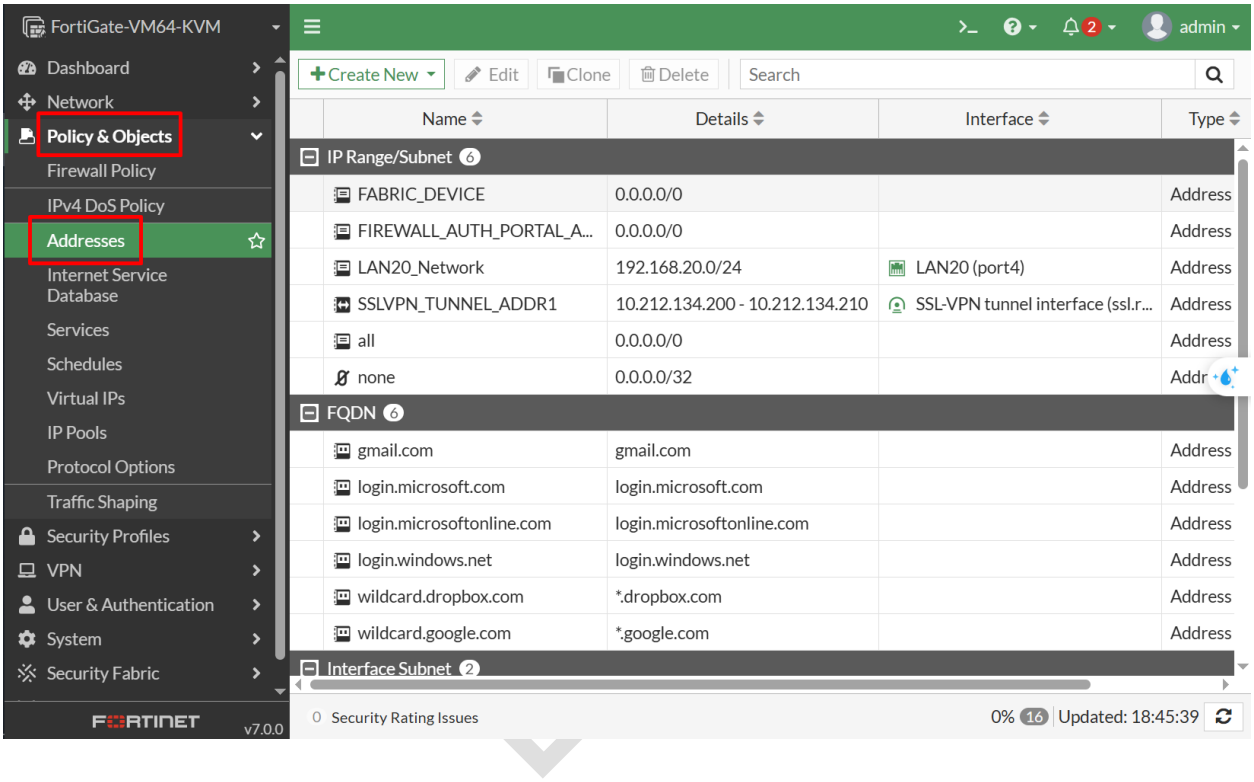


Kiểm tra hoạt động chính sách

Sau khi cấu hình xong Firewall Policy Allow_LAN_to_Internet, kiểm tra bằng cách mở trình duyệt trên máy tính thuộc mạng LAN. Nếu truy cập được Internet, chính sách đã hoạt động đúng.

3.2 Quản lý các đối tượng (Object Management)

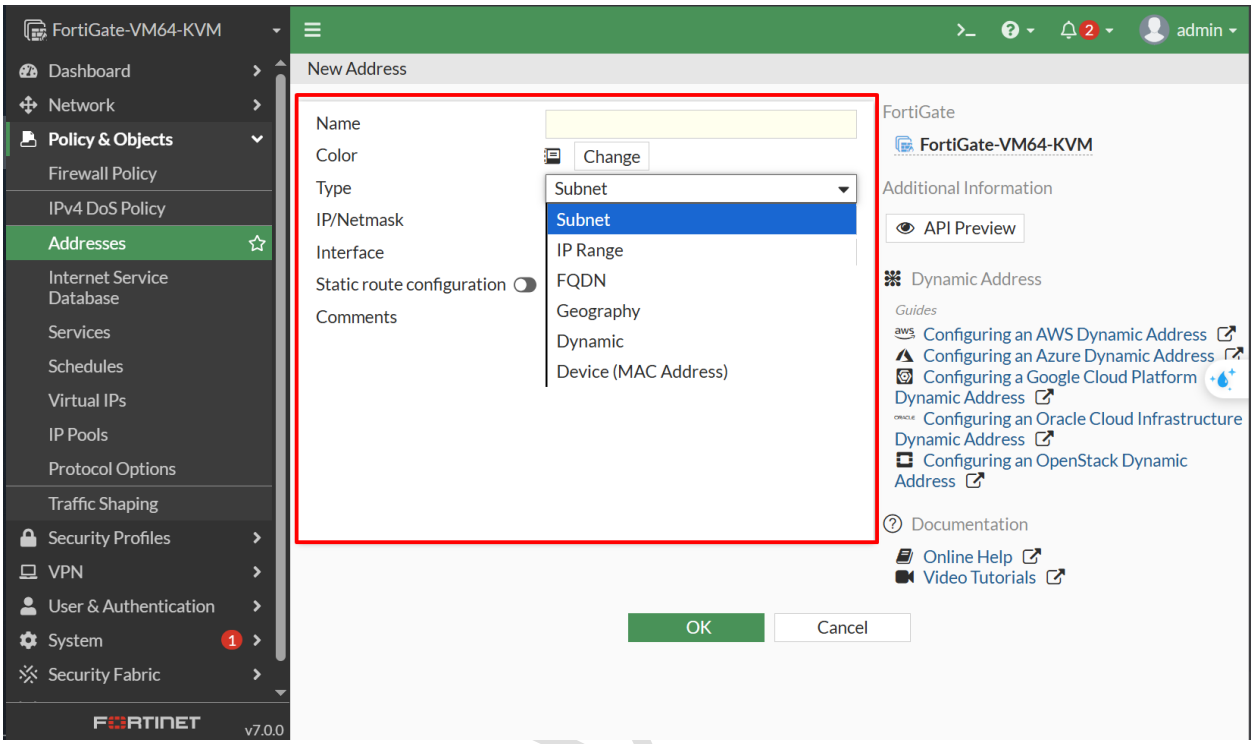
Để cấu hình chính sách tường lửa rõ ràng và dễ quản lý, chúng ta sử dụng khái niệm Object (đối tượng) trong FortiGate. Thay vì nhập địa chỉ IP hoặc thông số nhiều lần, chỉ cần tạo một đối tượng đại diện và sử dụng lại trong các policy khác nhau. Cách này giúp quản trị hệ thống thuận tiện, nhất là với hệ thống lớn hoặc nhiều chi nhánh.



Address Object (Địa chỉ)

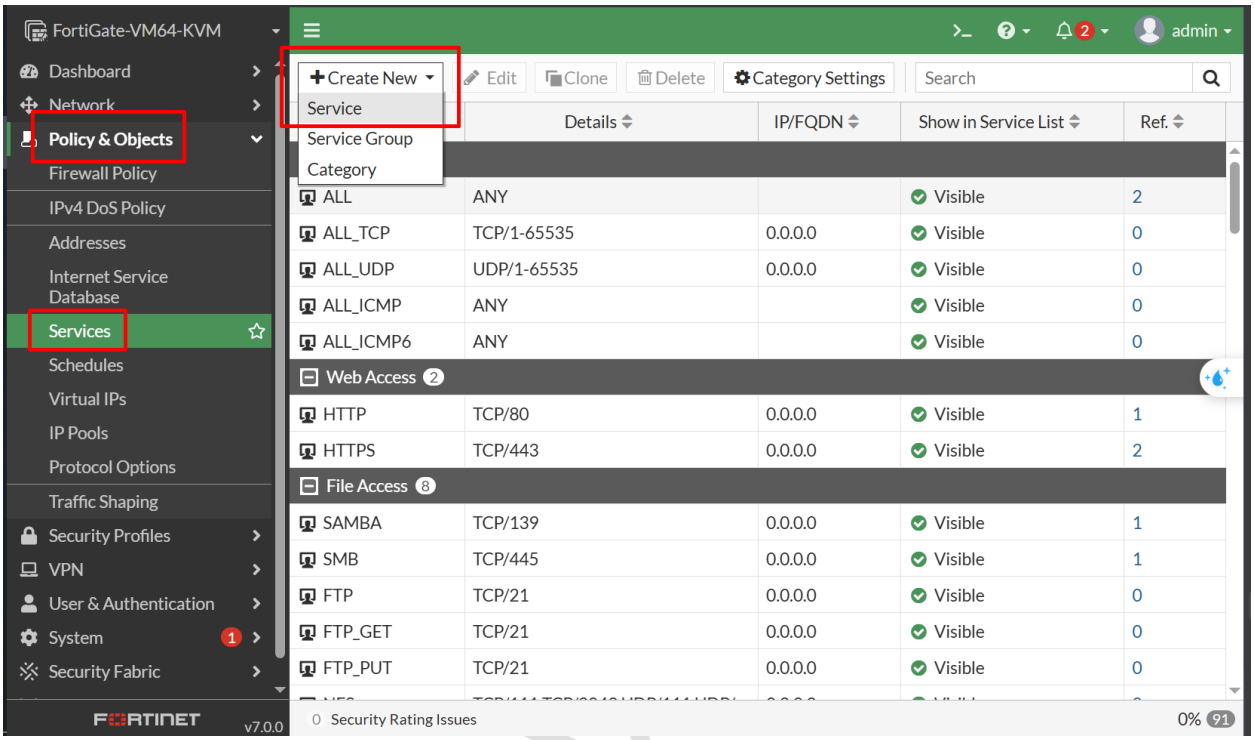
Address Object đại diện cho một địa chỉ IP hoặc một mạng. Để tạo mới, truy cập **Policy & Objects >**

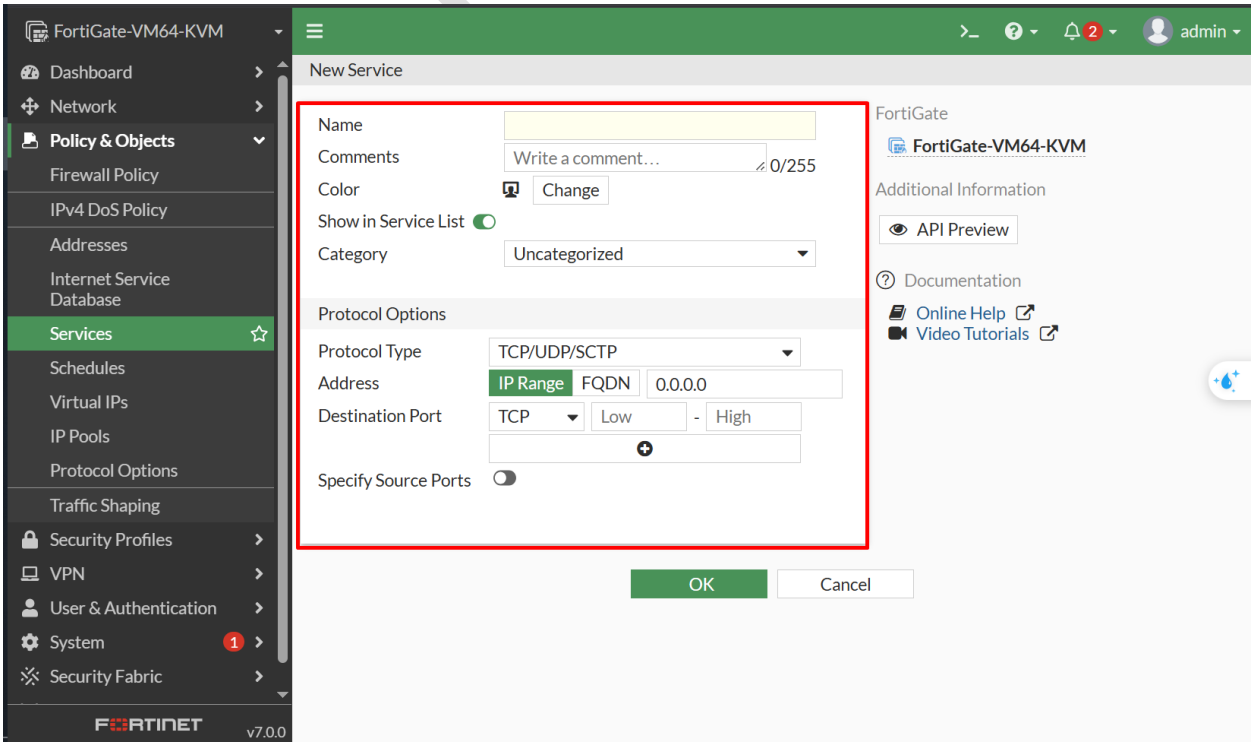
Addresses, chọn **Create New > Address** và điền thông tin.



Service Object (Dịch vụ)

Service Object đại diện cho một cổng (port) hoặc giao thức (protocol), giúp xác định loại lưu lượng mà policy sẽ áp dụng. Truy cập **Policy & Objects > Services** để quản lý các dịch vụ.

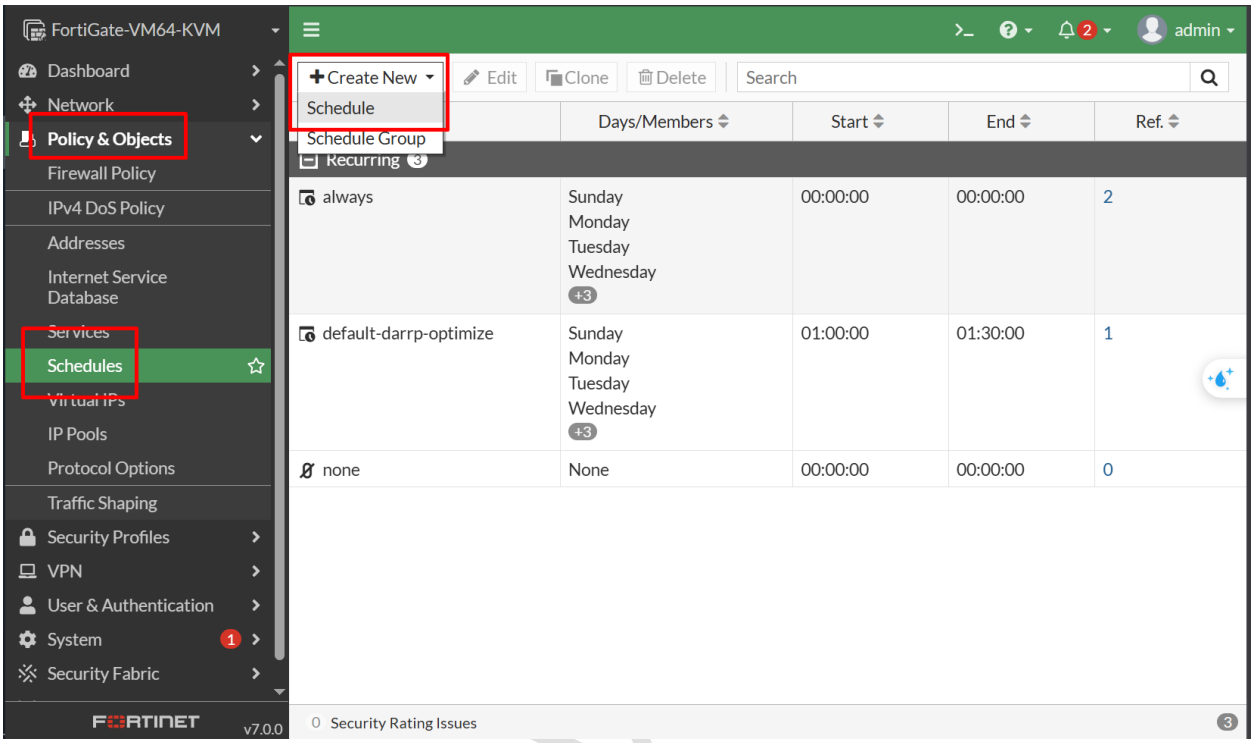


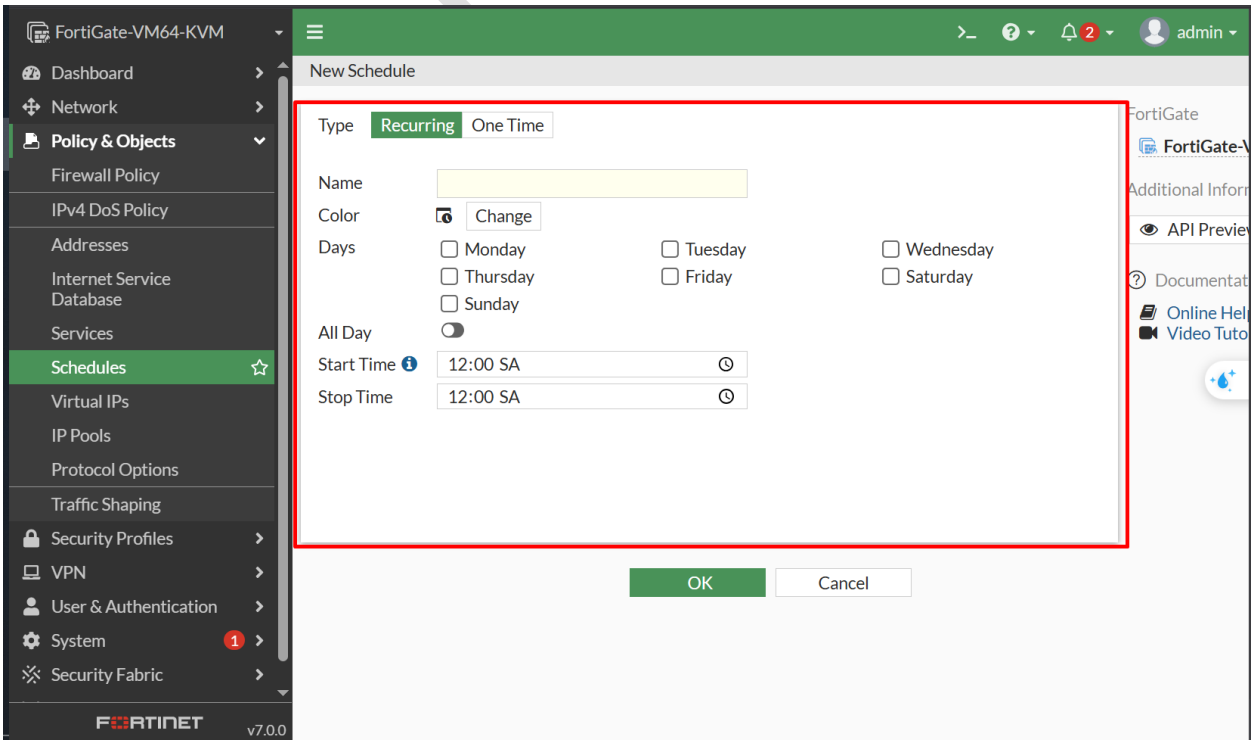


Schedule Object (Lịch biểu)

Schedule Object đại diện cho khoảng thời gian hoạt động của một policy. Truy cập **Policy & Objects >**

Schedules để tạo lịch biểu mới.





Tóm lại

Việc sử dụng các đối tượng (Objects) như Address, Service, Schedule giúp chúng ta cấu hình FortiGate rõ ràng, ngắn gọn và dễ tái sử dụng. Phương pháp này đặc biệt hiệu quả khi quản trị hệ thống lớn hoặc nhiều chi nhánh, đảm bảo tính nhất quán và thuận tiện vận hành.

4. Network Address Translation (NAT) và Virtual IPs (VIPs)

Trên môi trường Internet, địa chỉ IP công cộng (public IP address) là tài nguyên hạn chế và có giá trị cao. Phần lớn thiết bị trong mạng nội bộ (LAN) sử dụng địa chỉ IP riêng (private IP address, ví dụ: 192.168.x.x), các địa chỉ này không thể định tuyến trực tiếp ra Internet.

Chương này hướng dẫn cách FortiGate đóng vai trò cầu nối giữa hai phân vùng mạng thông qua kỹ thuật Network Address Translation (NAT).

4.1 NAT là gì? Khái niệm SNAT và DNAT

Network Address Translation (NAT) là quá trình thay đổi thông tin địa chỉ IP trong phần tiêu đề (header) của gói tin khi đi qua thiết bị như router hoặc firewall.

NAT gồm hai loại chính:

Bước 1. Source NAT (SNAT)

- SNAT chuyển đổi địa chỉ IP nguồn (source IP) từ địa chỉ riêng (private) sang địa chỉ công cộng (public).
- Dùng khi người dùng trong LAN cần truy cập Internet.
- Tất cả yêu cầu từ LAN sẽ xuất hiện trên Internet như đến từ một địa chỉ IP công cộng duy nhất của FortiGate.
- Phương pháp này giúp nhiều thiết bị nội bộ chia sẻ chung một kết nối Internet qua một địa chỉ IP công cộng.

Ví dụ: Máy tính 192.168.1.10 gửi gói tin ra Internet, FortiGate thay đổi IP nguồn thành 203.0.113.5 (IP công cộng của interface WAN).

Bước 2. Destination NAT (DNAT)

- DNAT chuyển đổi địa chỉ IP đích (destination IP) từ địa chỉ công cộng (public) sang địa chỉ riêng (private).
- Dùng khi người dùng từ Internet muốn truy cập máy chủ (web, mail, FTP, ...) trong LAN.
- FortiGate nhận gói tin với địa chỉ IP công cộng, sau đó chuyển tiếp (forward) đến máy chủ nội bộ phù hợp.
- Trên FortiGate, DNAT thực hiện qua đối tượng Virtual IP (VIP).

Ví dụ: Người dùng bên ngoài truy cập 203.0.113.5:80, FortiGate thực hiện DNAT đến 192.168.1.10:80 (máy chủ web nội bộ).

4.2 Cấu hình SNAT (Truy cập Internet)

Khi tạo Firewall Policy ở chương trước và kích hoạt NAT, chúng ta đã cấu hình thành công SNAT.

Tùy chọn "Use Outgoing Interface Address" cho phép FortiGate tự động sử dụng địa chỉ IP của cổng ra (WAN) làm địa chỉ nguồn (source address) cho tất cả lưu lượng đi ra Internet.

Đây là mô hình SNAT phổ biến nhất, còn gọi là Overload NAT hoặc PAT (Port Address Translation), cho phép nhiều IP nội bộ cùng chia sẻ một địa chỉ IP công cộng, phân biệt nhau bằng số hiệu cổng (port number).

Tóm lại:

- **SNAT**: LAN đi ra Internet (IP riêng → IP công cộng)
- **DNAT**: Internet truy cập vào LAN (IP công cộng → IP riêng)

FortiGate thực hiện đồng thời cả hai cơ chế này một cách tự động, an toàn và hiệu quả, giúp mạng nội bộ vừa kết nối Internet, vừa bảo toàn cấu trúc địa chỉ bên trong.

4.3 Cấu hình DNAT (Port Forwarding) bằng Virtual IP

Tình huống ví dụ (Case Study)

Ví dụ: Có một máy chủ CCTV trong LAN với địa chỉ IP 192.168.1.50. Yêu cầu truy cập hình ảnh CCTV từ Internet qua port 8080.

Các bước cấu hình chi tiết

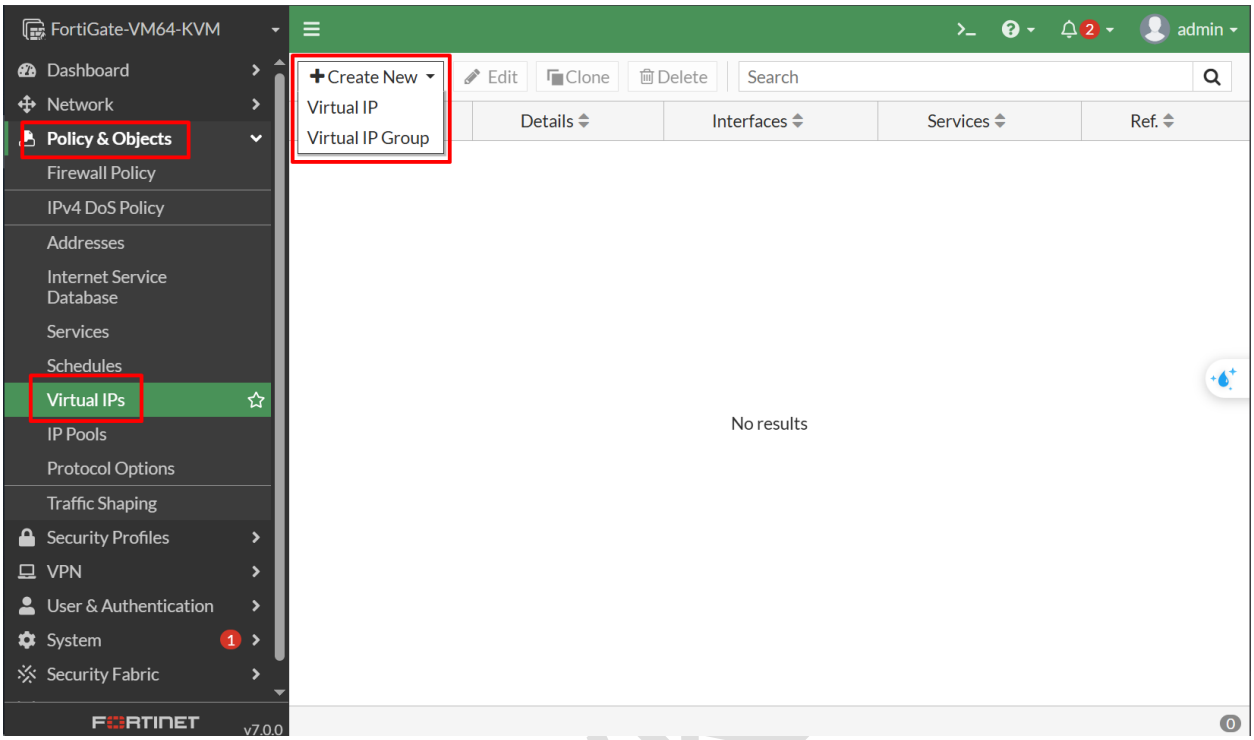
Bước 1. Tạo Virtual IP (VIP)

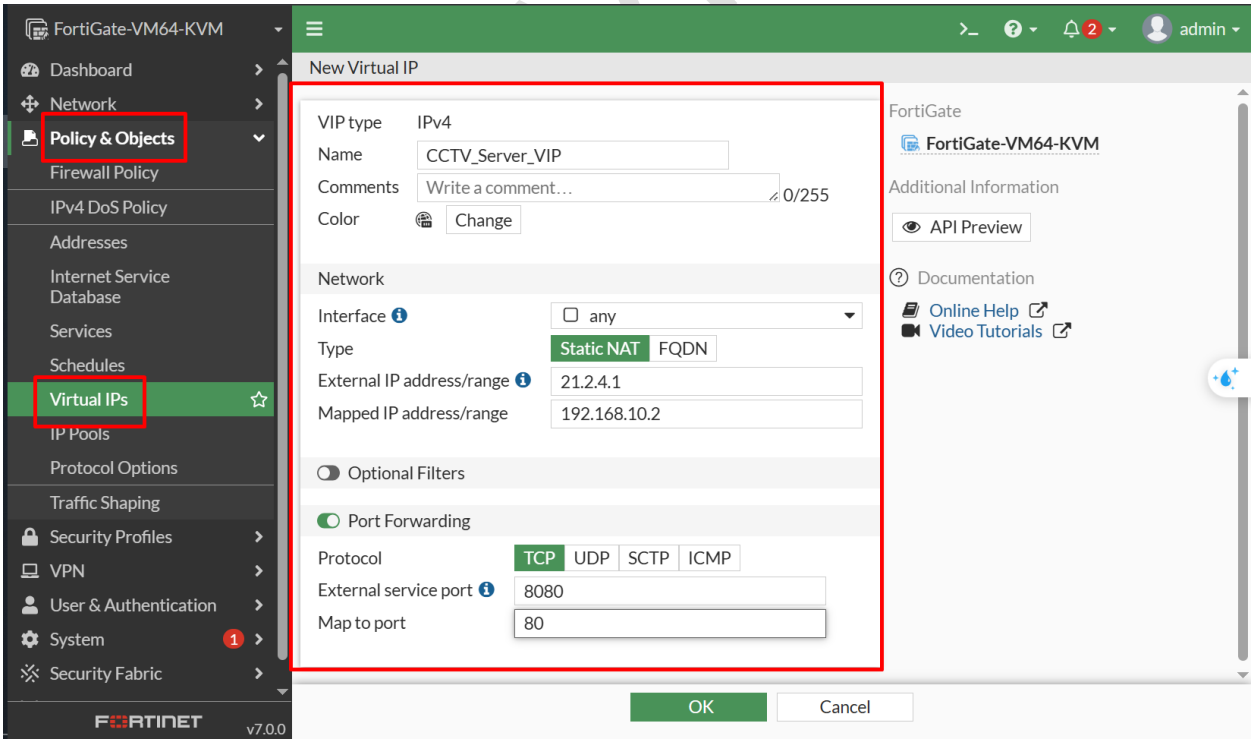
Mục đích: Ánh xạ (mapping) địa chỉ IP công cộng của FortiGate sang địa chỉ IP nội bộ của máy chủ.

Thao tác thực hiện:

- Vào **Policy & Objects > Virtual IPs**
- Chọn **Create New > Virtual IP**
- **Name**: CCTV_Server_VIP
- **External IP Address/Range**: Nhập địa chỉ IP công cộng của FortiGate (có thể chọn object đại diện cho interface WAN)
- **Mapped IP Address/Range**: Nhập 192.168.1.50 (địa chỉ nội bộ server CCTV)
- Bật Port Forwarding
- **Protocol**: TCP
- **External Service Port**: 8080 (port truy cập từ Internet)
- **Map to Port**: 80 (port dịch vụ CCTV chạy trong LAN)

- Nhấn **OK**


FortiGate-VM64-KVM
admin
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Create New
Virtual IP
Virtual IP Group
Edit
Clone
Delete
Search
Details
Interfaces
Services
Ref.
No results
FORTINET
v7.0.0

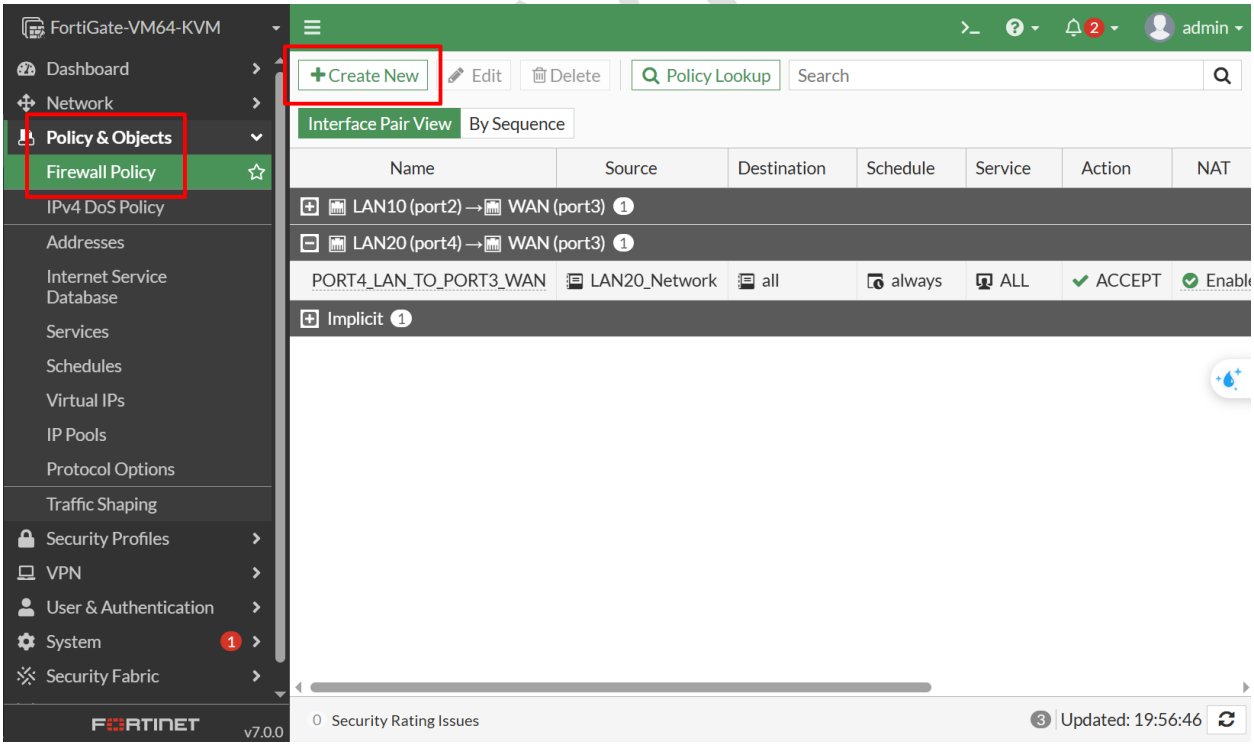

FortiGate-VM64-KVM
admin
New Virtual IP
VIP type IPv4
Name CCTV_Server_VIP
Comments Write a comment…
0/255
Color Change
Network
Interface any
Type Static NAT FQDN
External IP address/range 21.2.4.1
Mapped IP address/range 192.168.10.2
Optional Filters
Port Forwarding
Protocol TCP UDP SCTP ICMP
External service port 8080
Map to port 80
FortiGate
FortiGate-VM64-KVM
Additional Information
API Preview
Documentation
Online Help
Video Tutorials
OK
Cancel

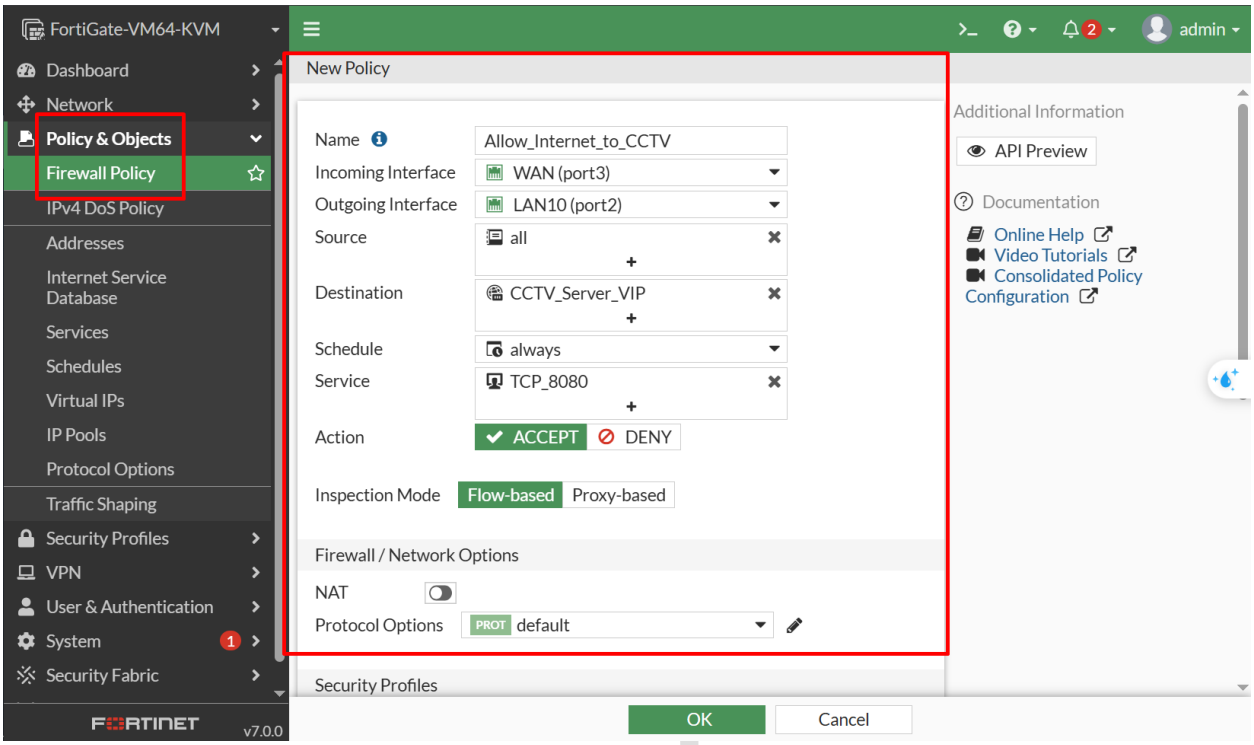
Bước 2. Tạo Firewall Policy cho phép truy cập

Mục đích: Cho phép lưu lượng từ Internet đi vào server nội bộ qua VIP vừa tạo.

Thao tác thực hiện:

- Vào **Policy & Objects > Firewall Policy**
- Chọn **Create New**
- **Name**: Allow_Internet_to_CCTV
- **Incoming Interface**: wan1 (cổng kết nối Internet)
- **Outgoing Interface**: lan (cổng nối về server CCTV)
- **Source**: all (mọi IP đều có thể truy cập — chỉ nên dùng khi kiểm thử, không khuyến nghị cấu hình thực tế)
- **Destination**: chọn object VIP CCTV_Server_VIP đã tạo
- **Service**: chọn TCP_8080 hoặc tạo custom service tương ứng với port forward
- **Action**: ACCEPT
- **Lưu ý quan trọng:** Tắt NAT (bỏ chọn NAT) vì FortiGate đã thực hiện DNAT bằng VIP, không cần SNAT thêm nữa
- Nhấn **OK**





Kiểm tra hoạt động

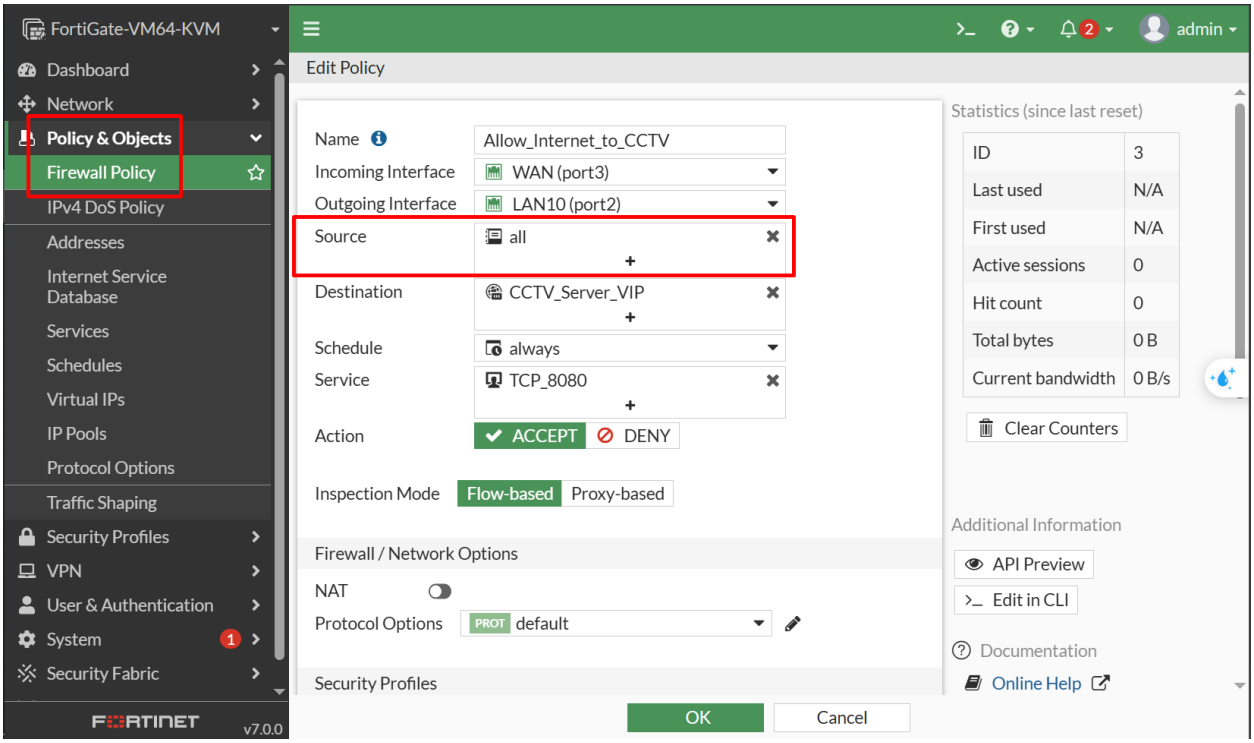
Từ mạng bên ngoài, mở trình duyệt và nhập URL truy cập. FortiGate sẽ nhận yêu cầu từ Internet, chuyển đổi IP đích sang 192.168.1.50, chuyển port 8080 về 80 và chuyển tiếp đến máy chủ CCTV.

Best Practices (Khuyến nghị bảo mật & tối ưu)

Mục tiêu: Hướng dẫn cấu hình NAT an toàn, dễ quản lý, giảm thiểu rủi ro khi mở truy cập từ Internet.

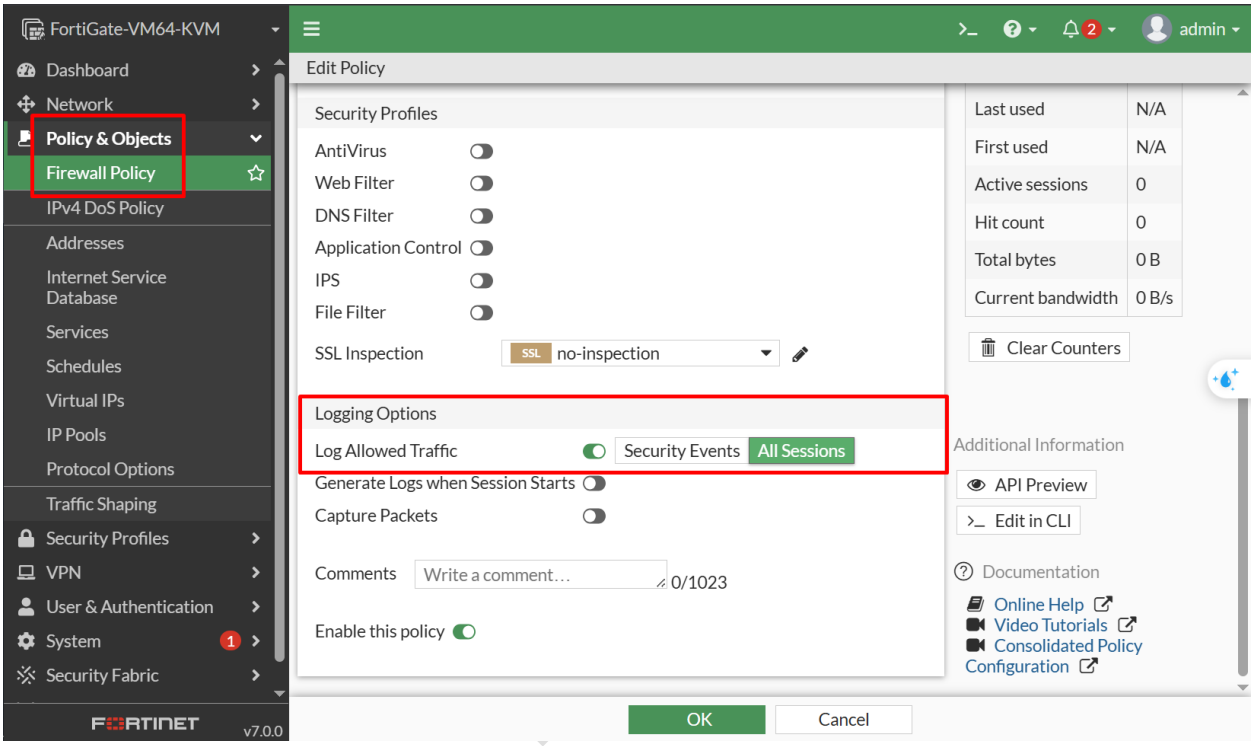
Bước 1. Không dùng "All Source" nếu không cần thiết

- Khi tạo Firewall Policy cho NAT (đặc biệt là DNAT/Port Forwarding), không nên đặt **Source** = all.
- Cấu hình này cho phép mọi IP trên Internet truy cập thiết bị hoặc dịch vụ nội bộ, tiềm ẩn rủi ro bảo mật.
- **Giải pháp:** Nếu chỉ cần truy cập từ văn phòng, chi nhánh, hoặc dải IP cố định, chỉ định cụ thể IP hoặc subnet. Ví dụ: Source: 203.113.5.0/24 (HeadOffice).
- Với truy cập tạm thời, có thể tạo Address Object riêng để quản lý linh hoạt.



Bước 2. Bật Logging để giám sát NAT

- Trong mỗi Firewall Policy, bật **Log Allowed Traffic** và chọn "All Sessions".
- **Mục đích:** Theo dõi địa chỉ IP nào được NAT ra Internet, phân tích lưu lượng DNAT (xác định ai truy cập dịch vụ nội bộ), hỗ trợ kiểm tra khi có sự cố hoặc dấu hiệu tấn công.
- Thao tác: **Policy & Objects > Firewall Policy > Edit Policy → Log Allowed Traffic: Enable (All Sessions)**

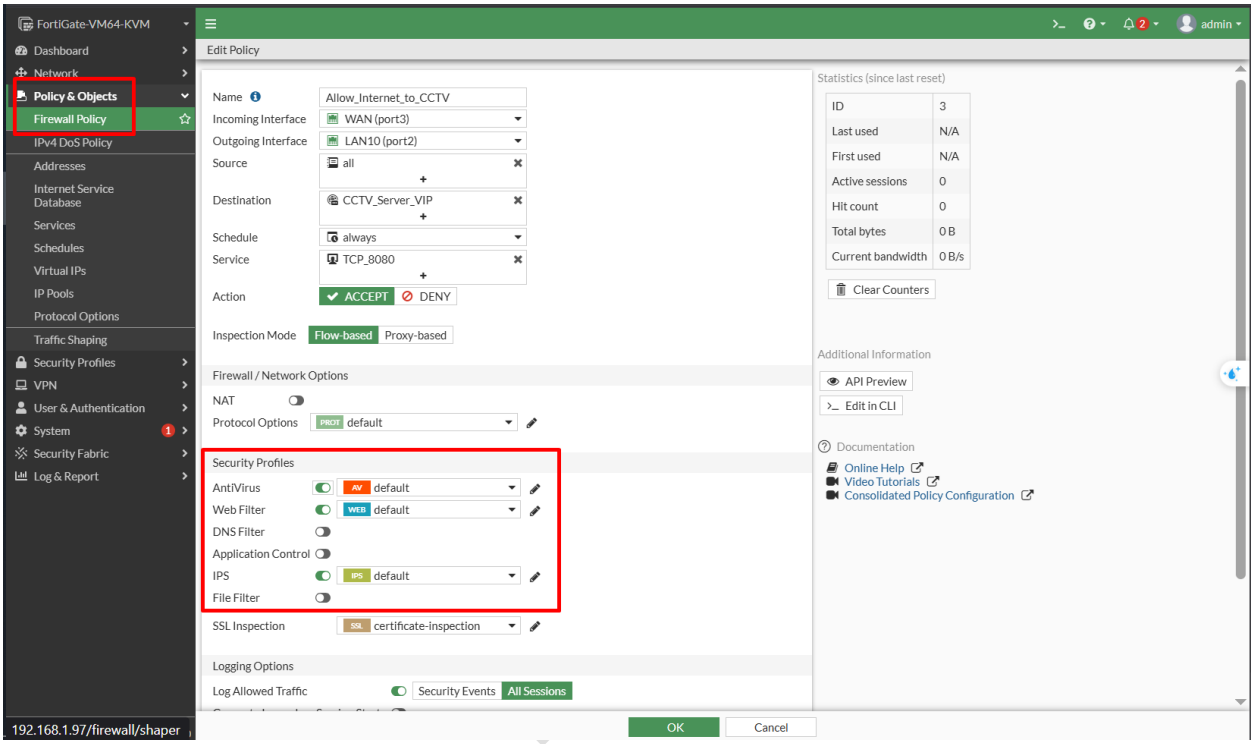


Bước 3. Giới hạn quyền truy cập theo nguyên tắc "Least Privilege"

- NAT Policy chỉ nên cho phép đúng thành phần cần thiết:
- **Nguồn (Source):** Địa chỉ hoặc dải IP cần thiết.
- **Dịch vụ (Service/Port):** Chỉ các dịch vụ cần thiết.
- **Lịch biểu (Schedule):** Áp dụng nếu cần giới hạn thời gian hoạt động.
- Ví dụ: Server FTP chỉ hoạt động trong giờ hành chính, có thể áp dụng Schedule: Office_Hours.

Bước 4. Thêm lớp bảo vệ

- Với **DNAT (Inbound)**: Luôn bật các Security Profiles (IPS, Antivirus, Web Filter) để bảo vệ máy chủ nội bộ.
- Với **SNAT (Outbound)**: Nên bật Web Filter, Application Control để giám sát và kiểm soát truy cập ra ngoài.
- Giải pháp này bảo vệ hệ thống ở cả hai chiều lưu lượng.



5. Security Profiles và Bảo mật cơ bản

Khái niệm về Security Profiles

Trong hệ thống Fortinet Firewall, **Security Profiles** là lớp bảo vệ bổ sung, giúp kiểm soát không chỉ truy cập mà còn nội dung và hành vi của dữ liệu đi qua tường lửa. Firewall Policy giống như nhân viên gác cổng, kiểm tra thẻ ID (địa chỉ IP và cổng) của người ra vào. Nếu thông tin hợp lệ, được phép đi qua. Security Profiles là lớp kiểm tra bảo mật thứ hai nằm sau cổng, như máy dò kim loại hoặc máy quét hành lý, nhằm phát hiện các nguy cơ tiềm ẩn bên trong dữ liệu. Mỗi Security Profile (ví dụ: Antivirus, Web Filter, Application Control...) có thể cấu hình độc lập và gắn vào một hoặc nhiều Firewall Policy để tăng cường bảo vệ hệ thống.

- – **Firewall Policy**: kiểm tra “ai được vào” (địa chỉ IP, cổng dịch vụ).
- – **Security Profile**: kiểm tra “mang gì vào” (nội dung, file, ứng dụng,...).

Kết hợp cả hai giúp kiểm soát truy cập và bảo vệ hệ thống trước các mối đe dọa tiềm ẩn từ bên trong gói tin.

Cấu hình các Tính năng Bảo mật Cơ bản

Dưới đây là các bước cấu hình những Security Profile phổ biến nhất trên FortiGate. Thao tác tại mục **Security Profiles** trên menu trái giao diện quản trị.

Antivirus (AV)

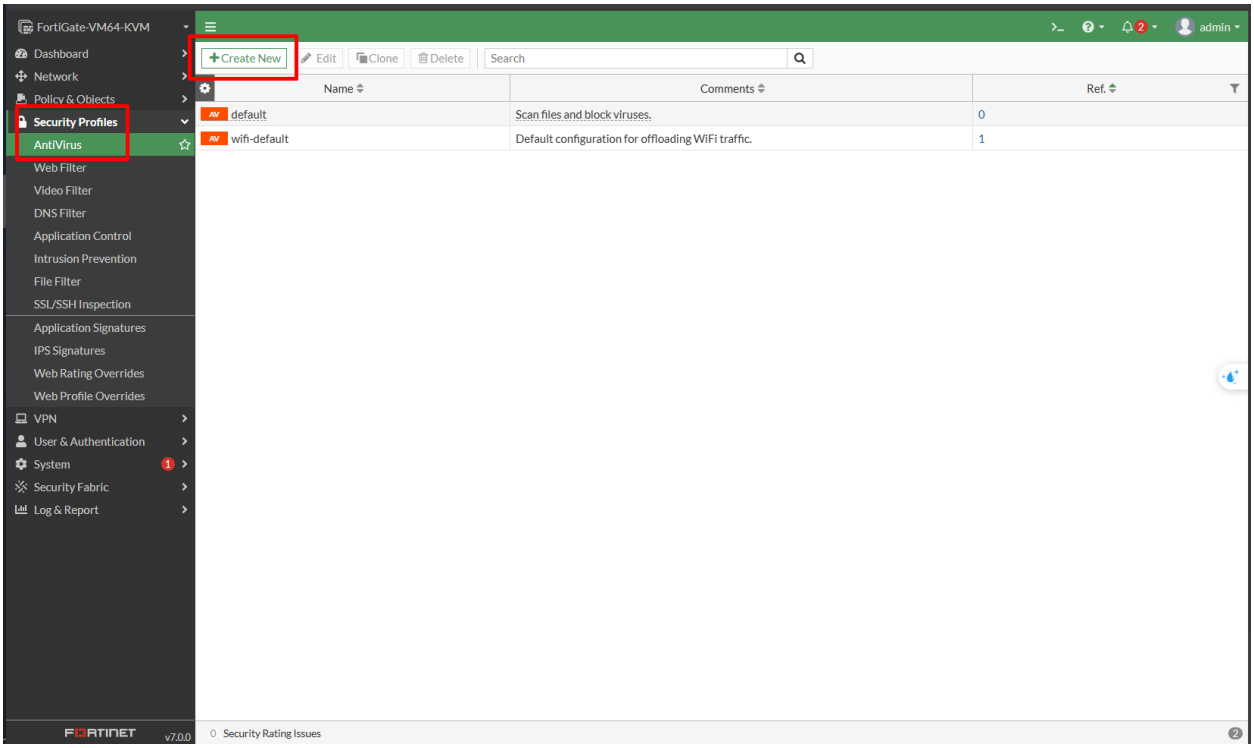
Bước 1: Vào **Security Profiles > AntiVirus**.

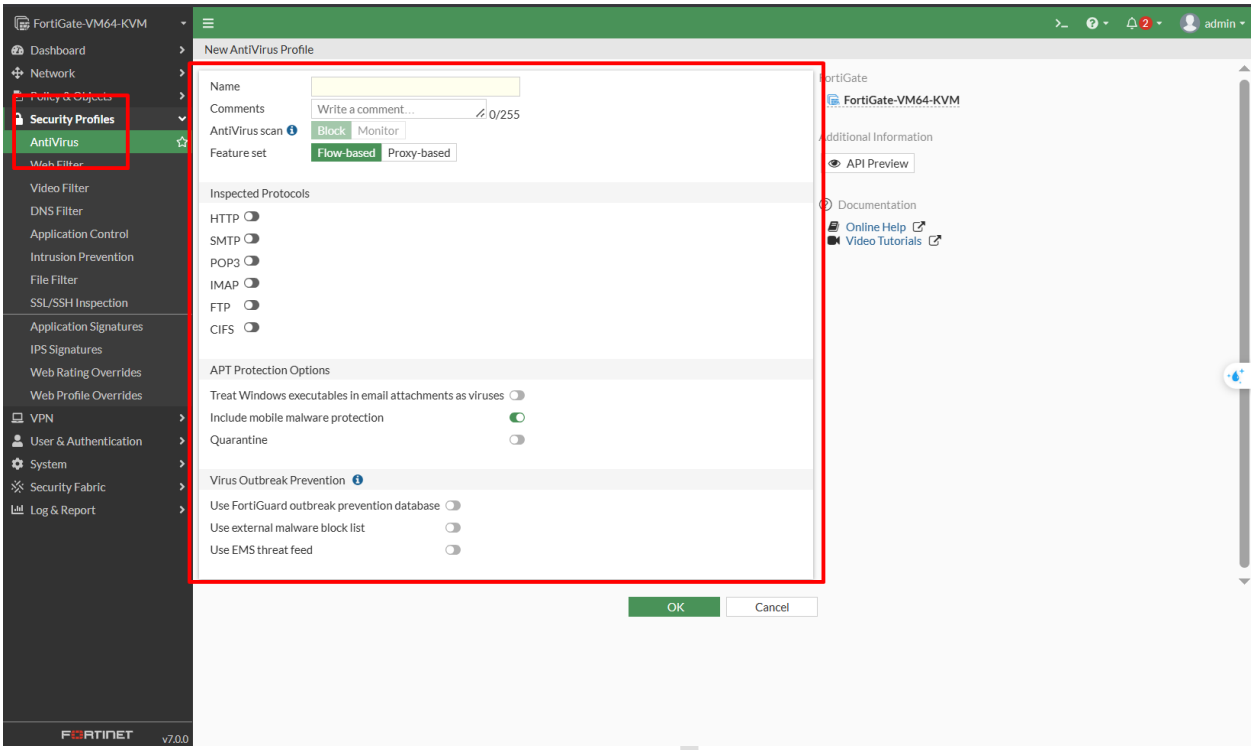
Bước 2: Chúng ta sẽ thấy profile mặc định (default profile) – có thể chỉnh sửa (Edit) hoặc tạo mới (Create New).

Bước 3: Trong phần cấu hình, đảm bảo **Scan Files** đang được bật.

Bước 4: Chọn các giao thức cần quét như **HTTP, FTP, Email...**

- – Chức năng: Quét và ngăn chặn file độc hại, virus hoặc mã độc trong luồng dữ liệu.





Ví dụ thử nghiệm với EICAR:

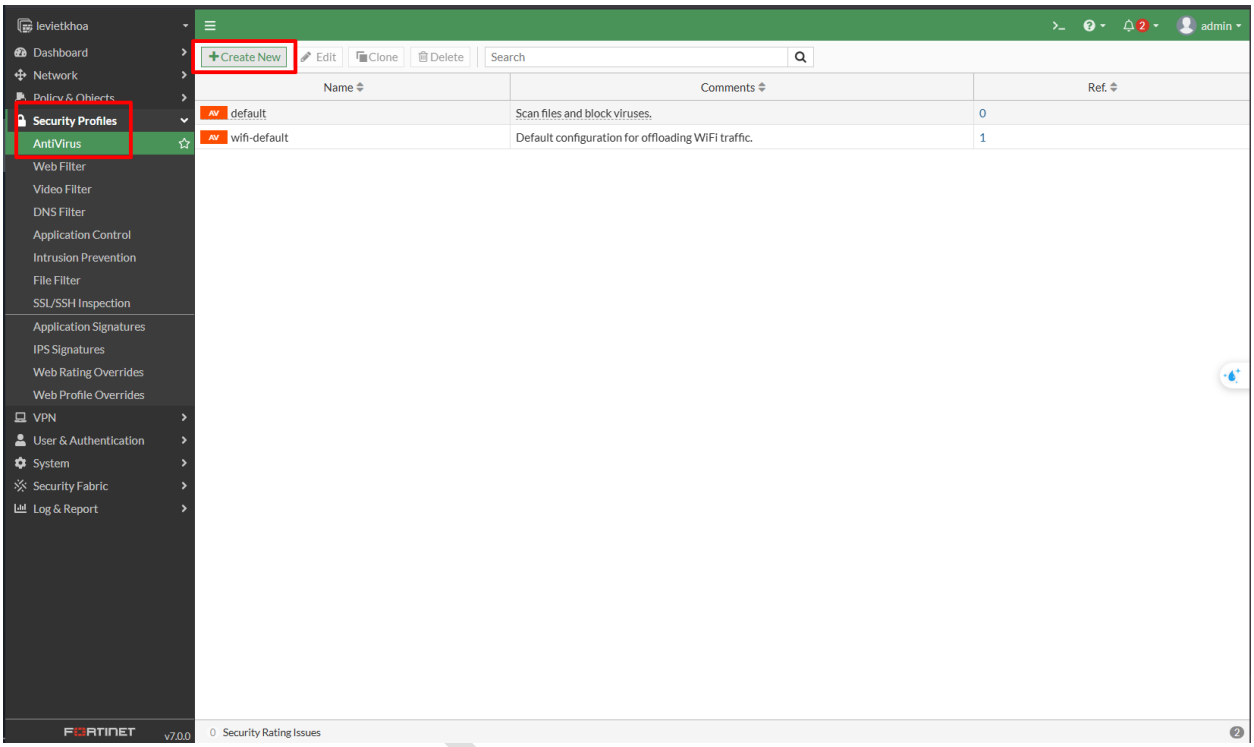
Tệp EICAR là một tệp kiểm tra an toàn được tạo ra bởi Viện Nghiên cứu Chống Virus Máy tính Châu Âu (EICAR) để kiểm tra hoạt động của phần mềm diệt virus và phần mềm chống phần mềm độc hại. Nó không phải là một virus thực sự, mà là một đoạn mã văn bản được thiết kế để bị các chương trình bảo mật nhận diện là một mối đe dọa, từ đó xác minh rằng phần mềm đang hoạt động đúng cách.

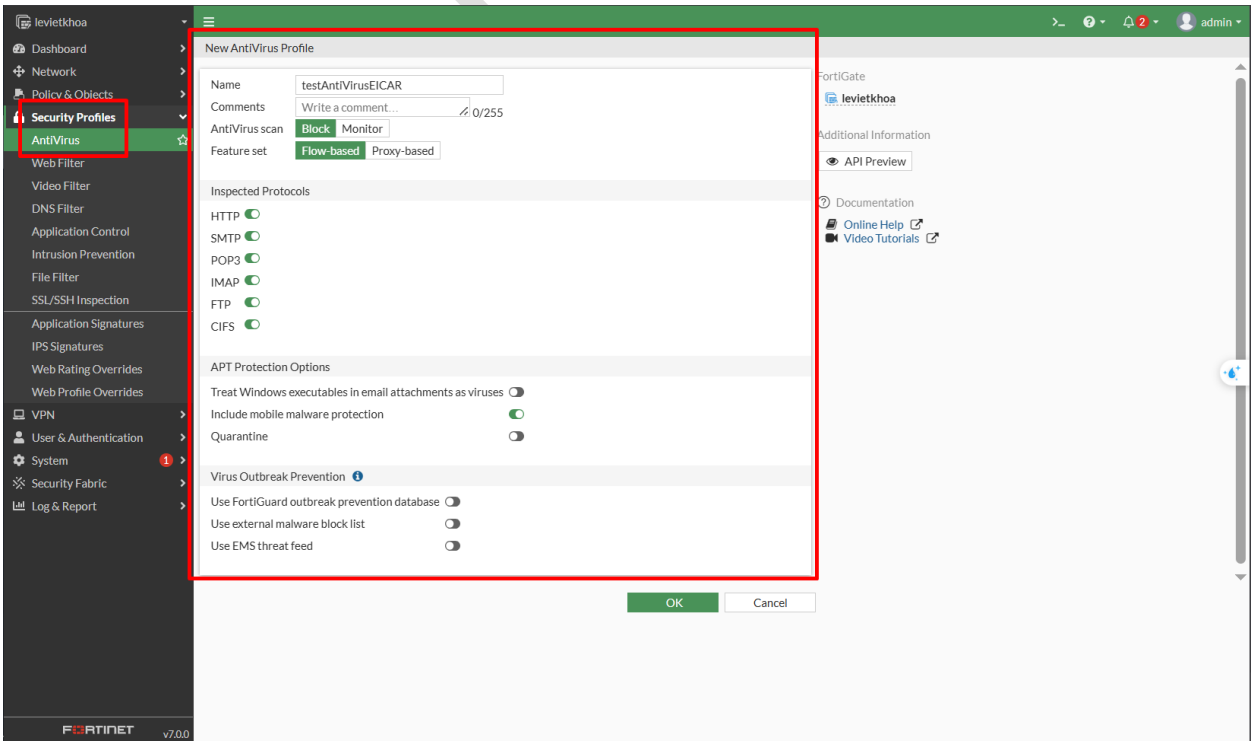
Tại sao tệp EICAR lại quan trọng?

Kiểm tra hiệu quả:

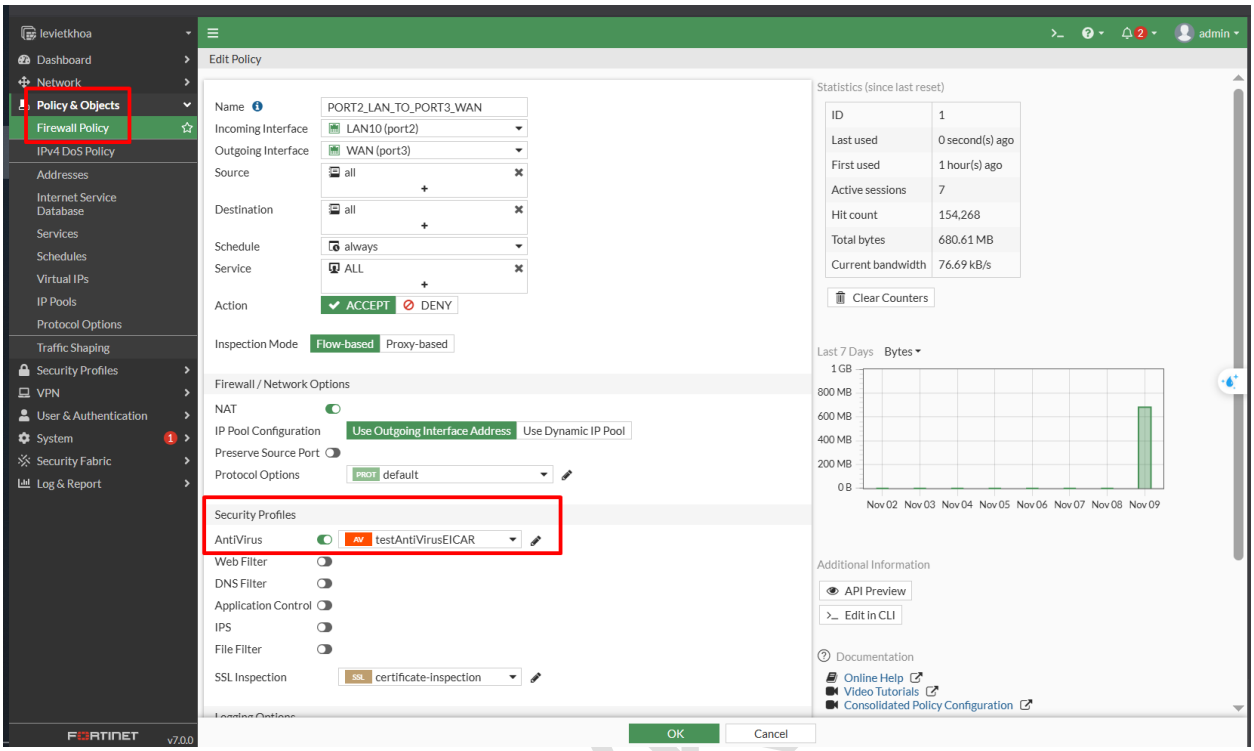
Tệp EICAR cho phép người dùng và quản trị viên hệ thống kiểm tra xem phần mềm diệt virus của họ có hoạt động chính xác để phát hiện và chặn các mối đe dọa hay không.

- – Truy cập **Security Profiles - AntiVirus**, tạo mới AV:
    - – Tên: testAntiVirusEICAR
    - – Detect Viruses: Block
    - – Inspected Protocols: HTTP, SMTP, POP3, IMAP, FTP, CIFS

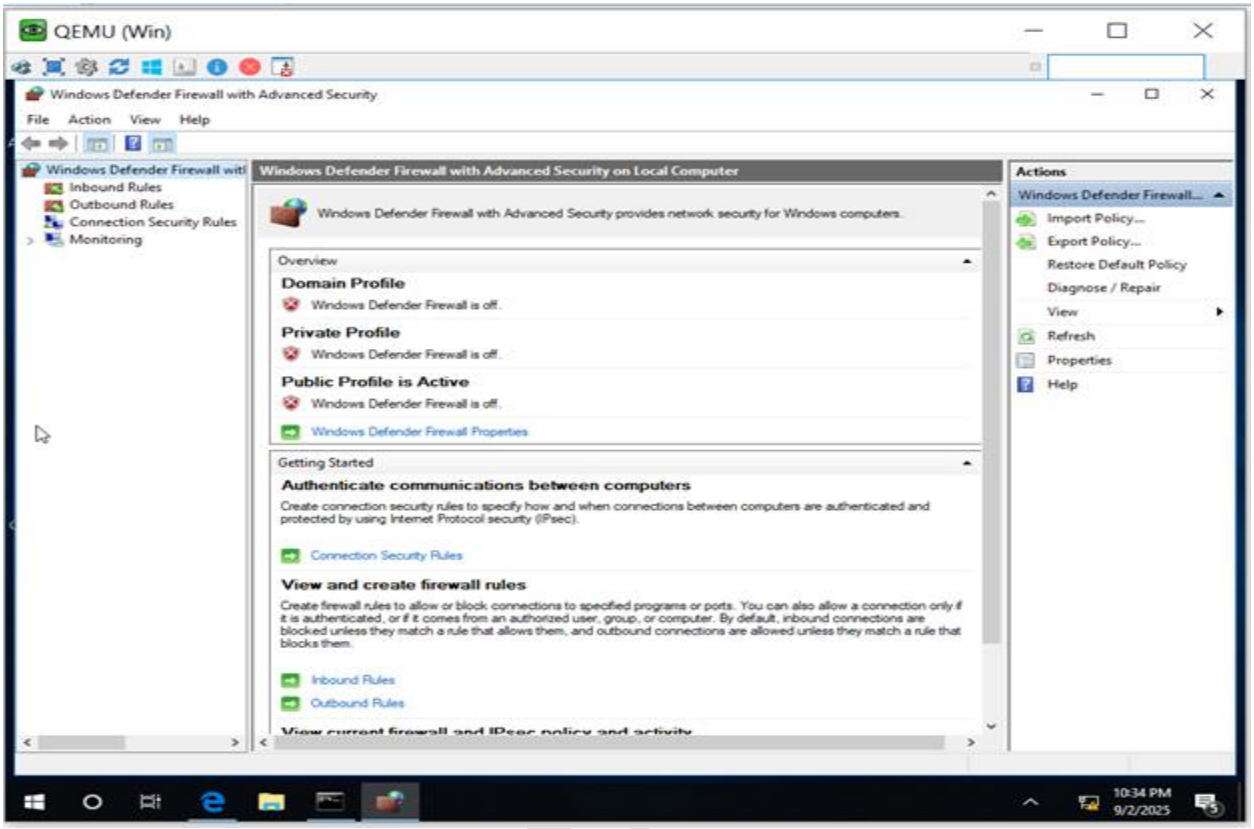


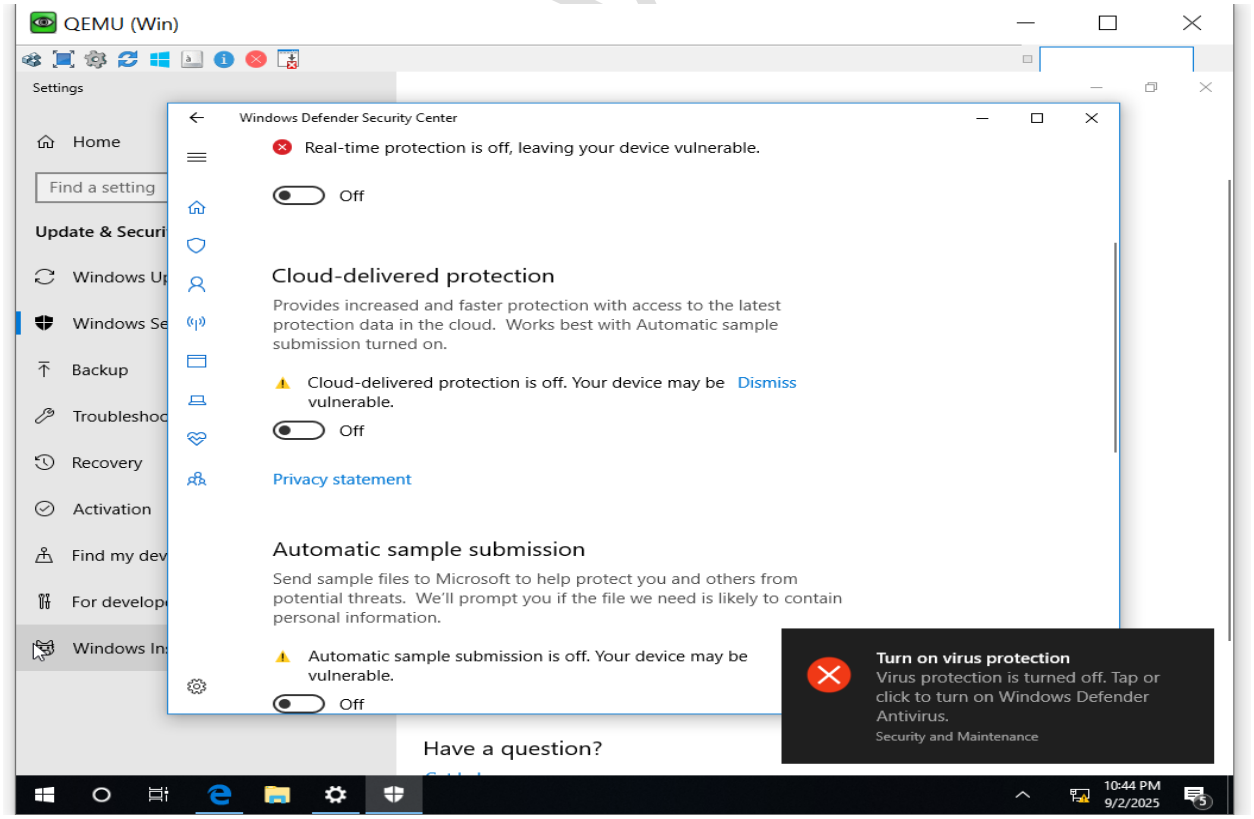


- – Thêm AV mới tạo vào policy **PORT_2_LAN_TO_PORT_3_WAN**.

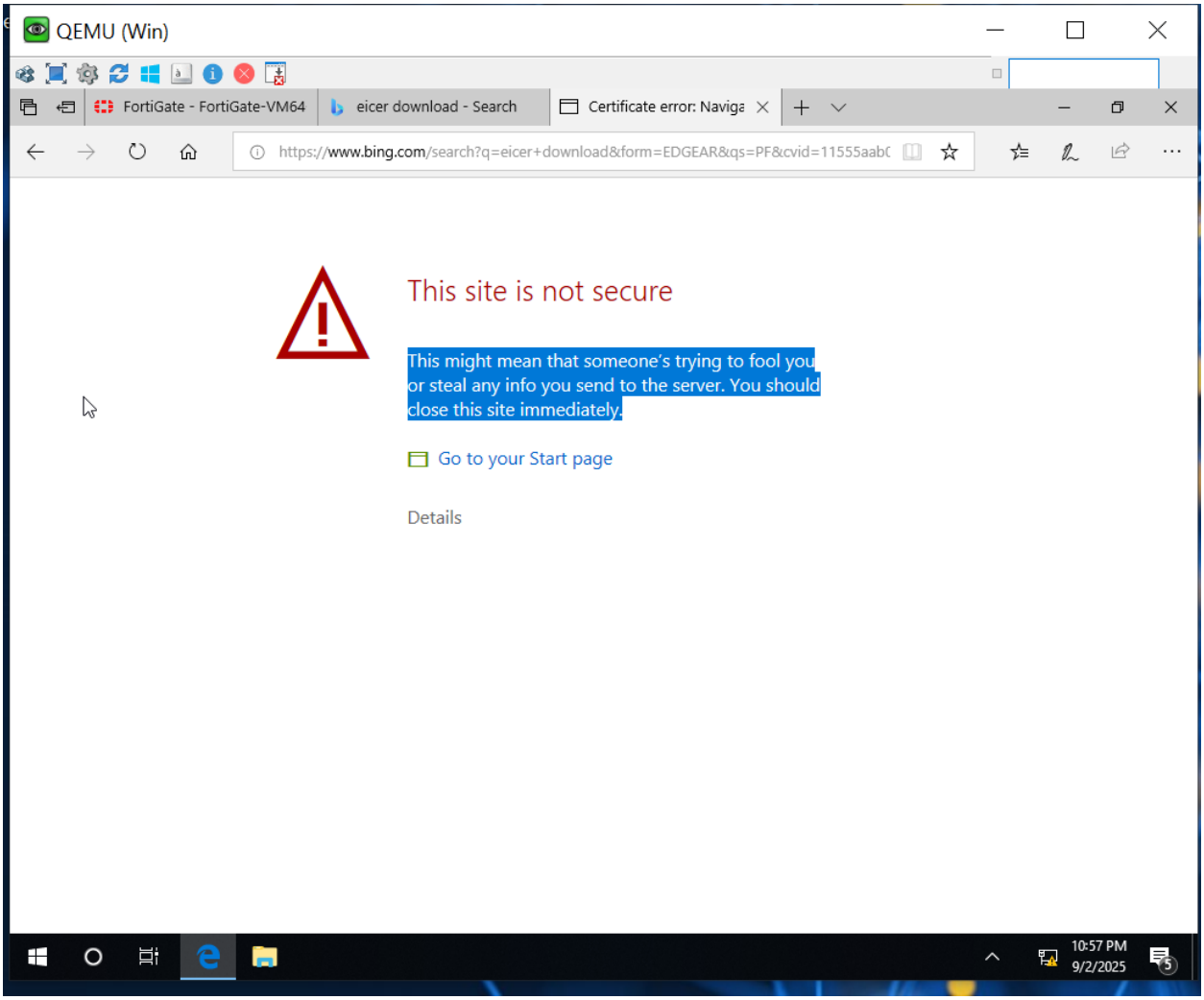


- – Tắt Windows Defender trên máy thử nghiệm để kiểm tra hiệu quả của FortiGate Antivirus.





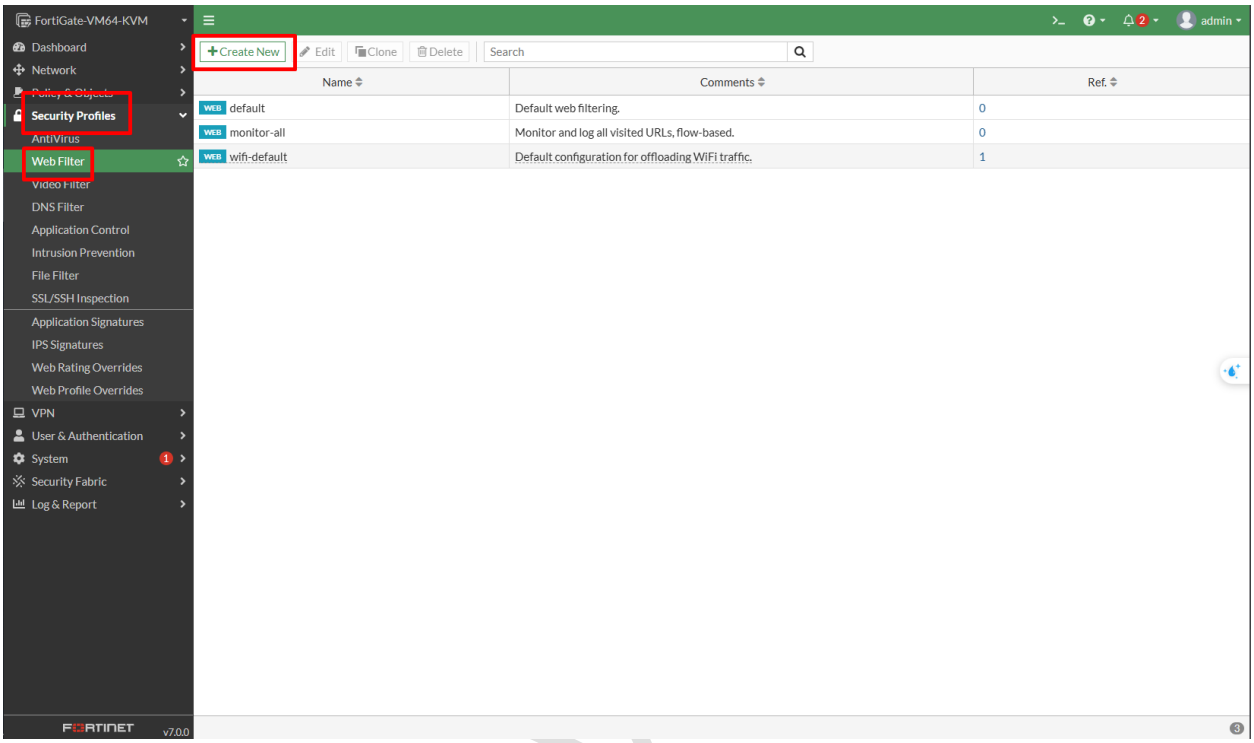
Kết quả: Dù đã tắt Windows Defender, chúng ta không thể download được file EICAR về máy, chứng tỏ Antivirus trên FortiGate đã hoạt động.



Web Filter

Bước 1: Vào **Security Profiles > Web Filter**.

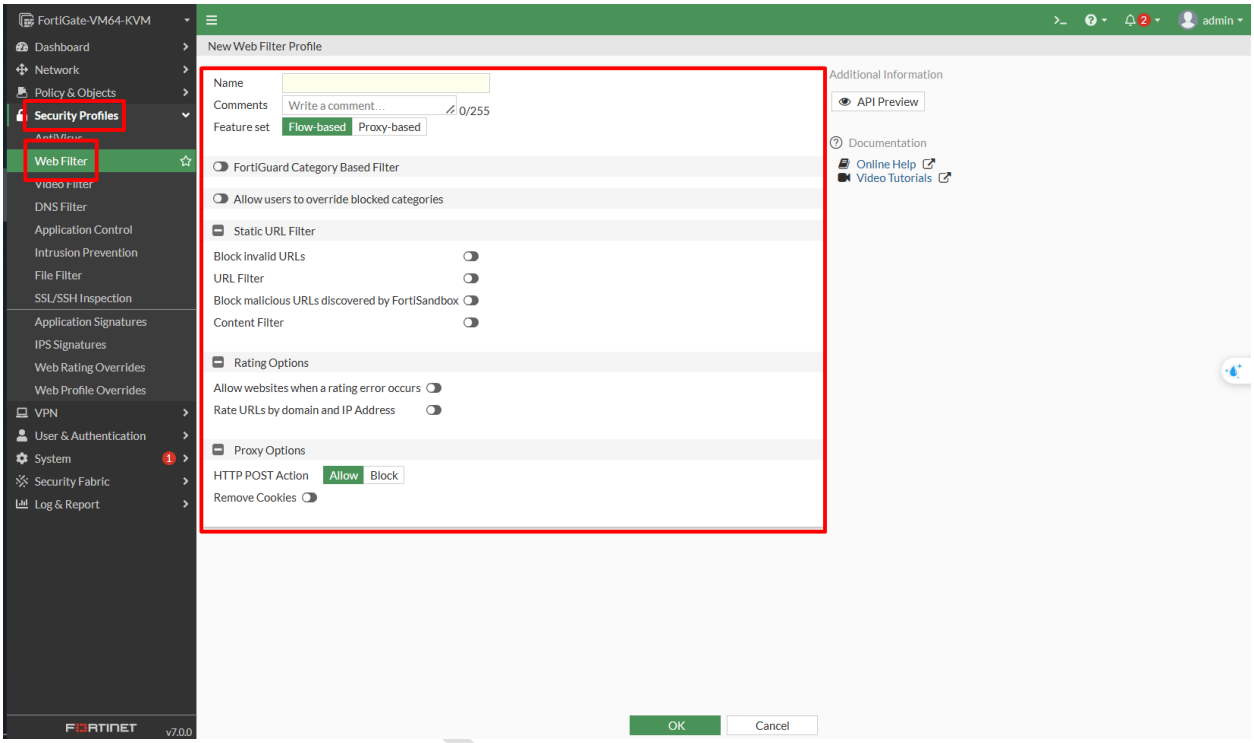
Bước 2: Chỉnh sửa profile mặc định hoặc **Create New** để tạo mới.



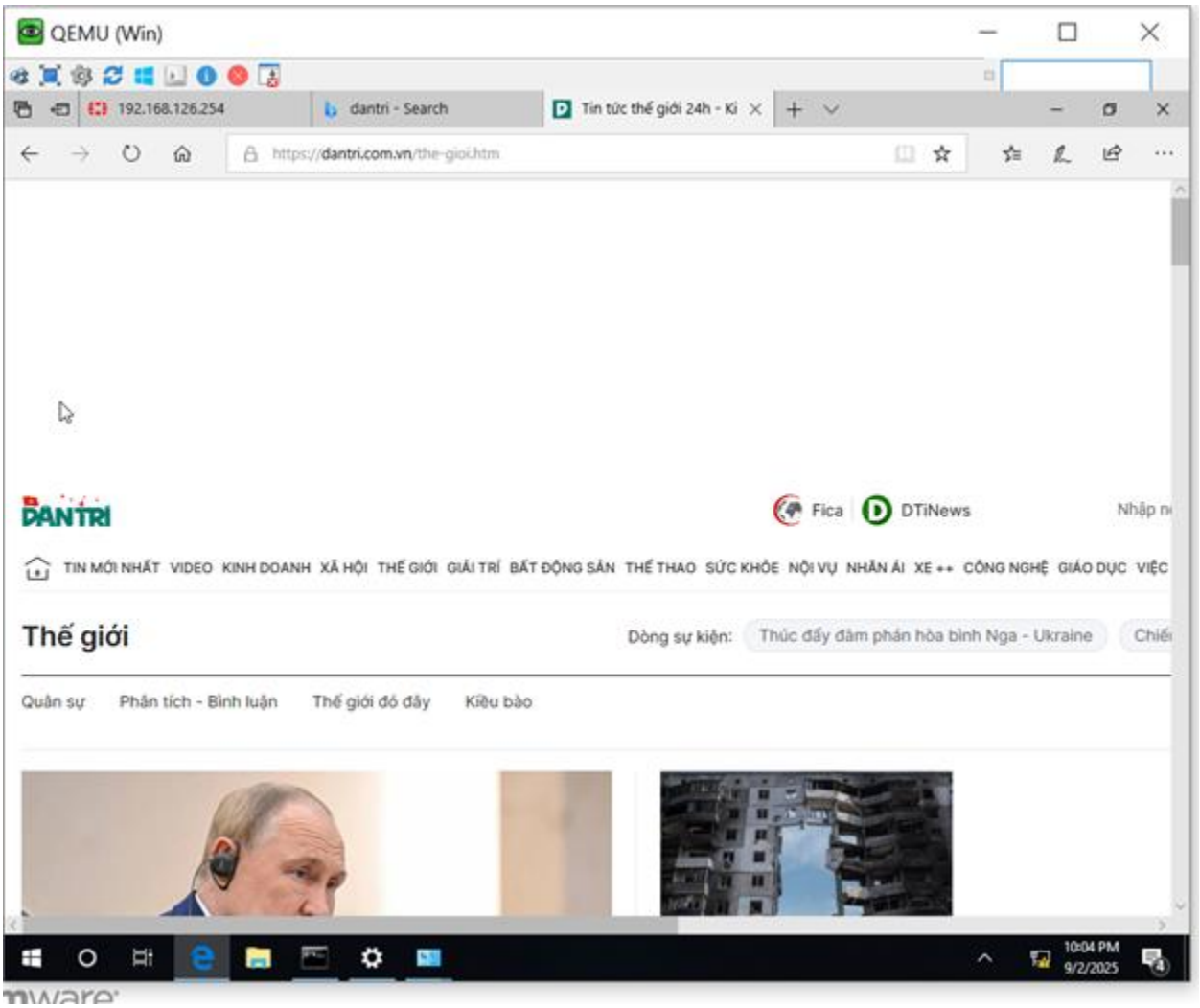
Bước 3: Tại đây có danh sách các **FortiGuard Category Filters** – nơi có thể chặn nhóm website.

- – Ví dụ: Tìm nhóm **Bandwidth Consuming** → Block (chặn các trang video streaming).
- – Tìm nhóm **Malicious Websites** → đảm bảo đặt ở chế độ Block.

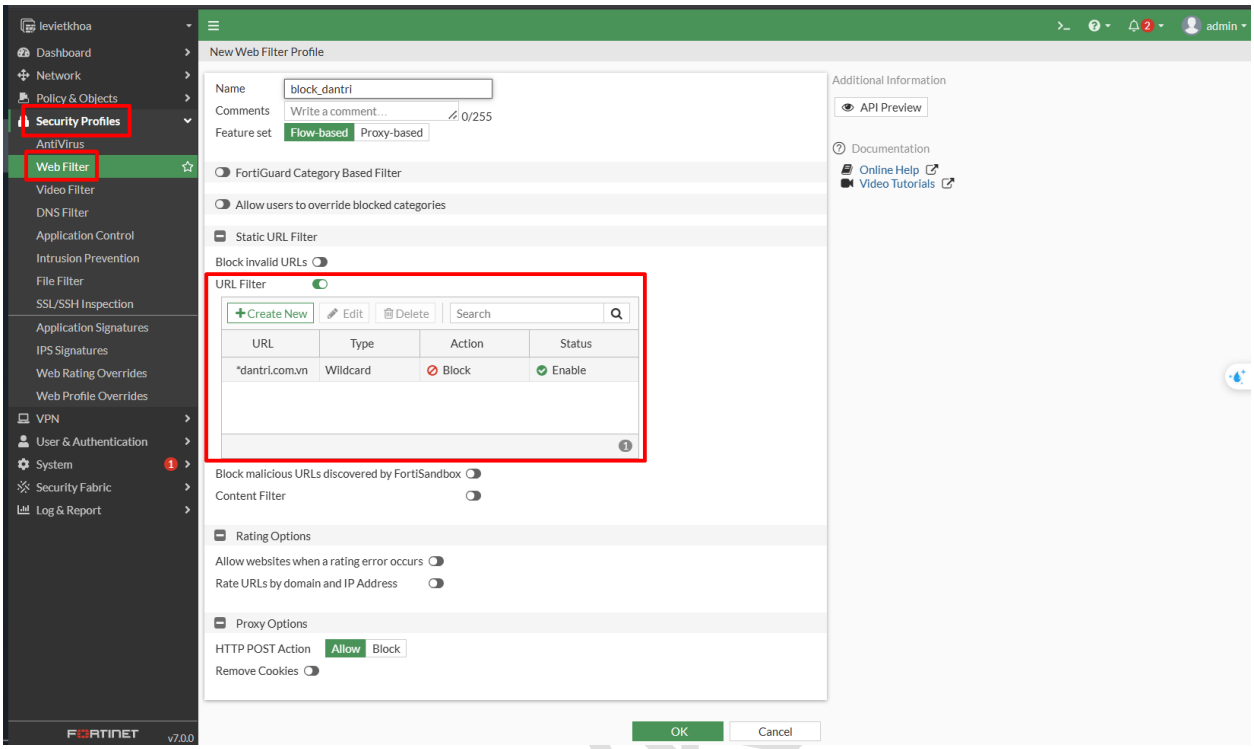
– Chức năng: Ngăn người dùng truy cập website độc hại hoặc ngoài chính sách công ty.



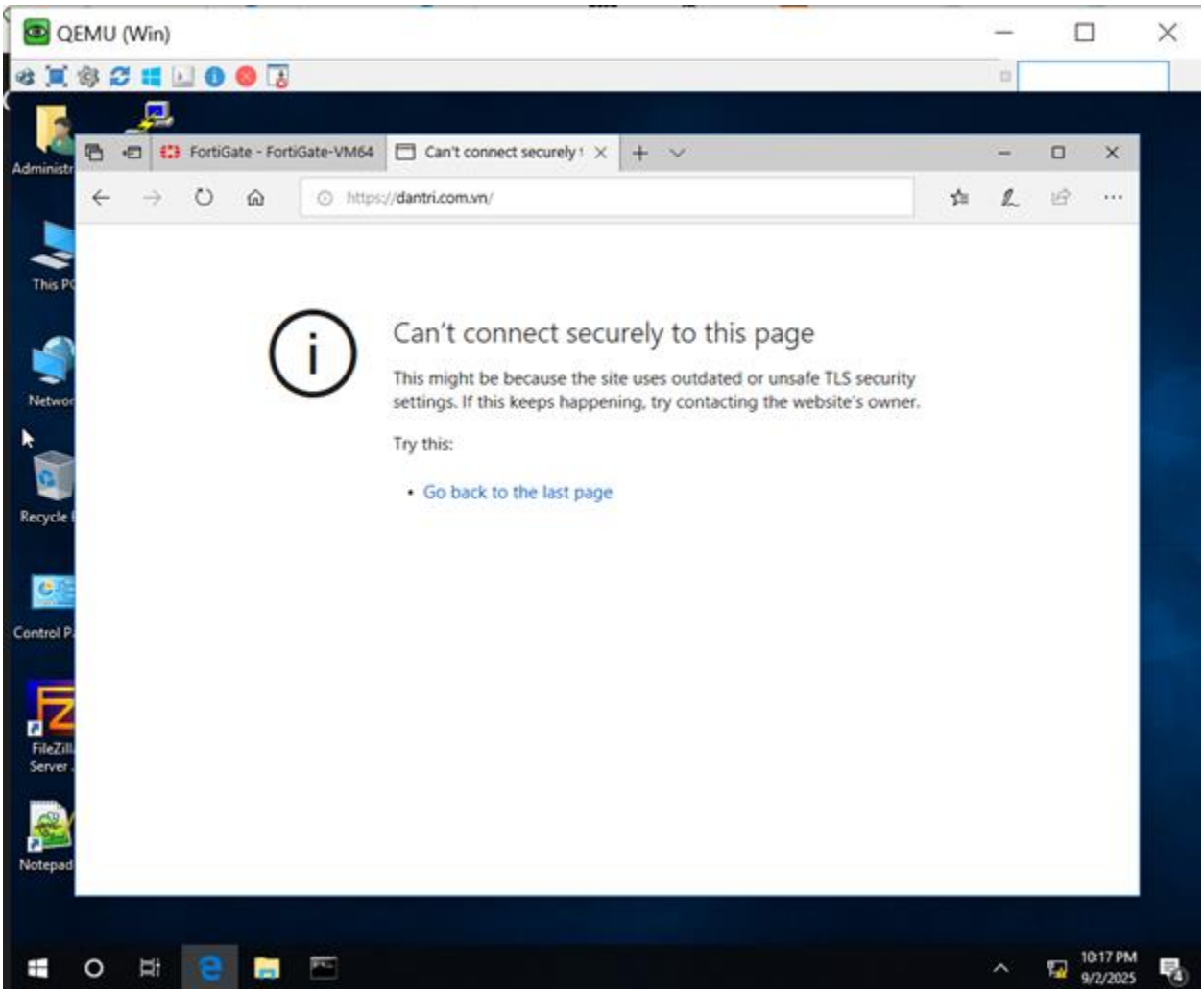
Ví dụ: Nếu không cấu hình, chúng ta có thể truy cập dantri.com.



Sau khi truy cập **Security Profiles – Web Filter** và chặn URL của ***dantri.com.vn**



User LAN sẽ không truy cập được dantri.



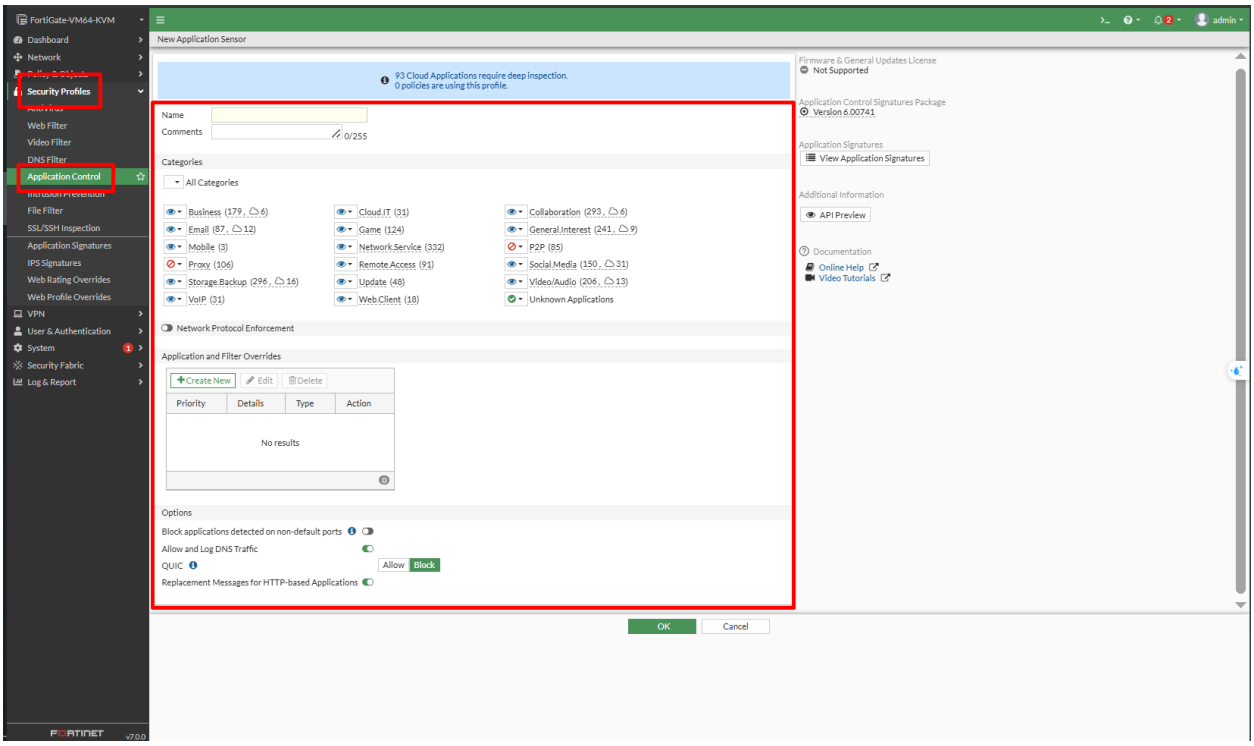
Application Control

Bước 1: Vào **Security Profiles > Application Control**.

Bước 2: Tính năng này cho phép kiểm soát ứng dụng, không chỉ website.

Bước 3: Trong phần **Application and Filter Overrides**, nhấn **Create New**:

- – Tại **Application**, nhập “BitTorrent”.
- – Chọn ứng dụng → **Action**: Block. Kết quả: ngăn toàn bộ người dùng sử dụng BitTorrent trong mạng nội bộ.



– Chức năng: Quản lý và giới hạn các ứng dụng theo chính sách bảo mật (VD: chặn game, P2P,...).

Intrusion Prevention System (IPS)

Bước 1: Vào **Security Profiles > Intrusion Prevention**.

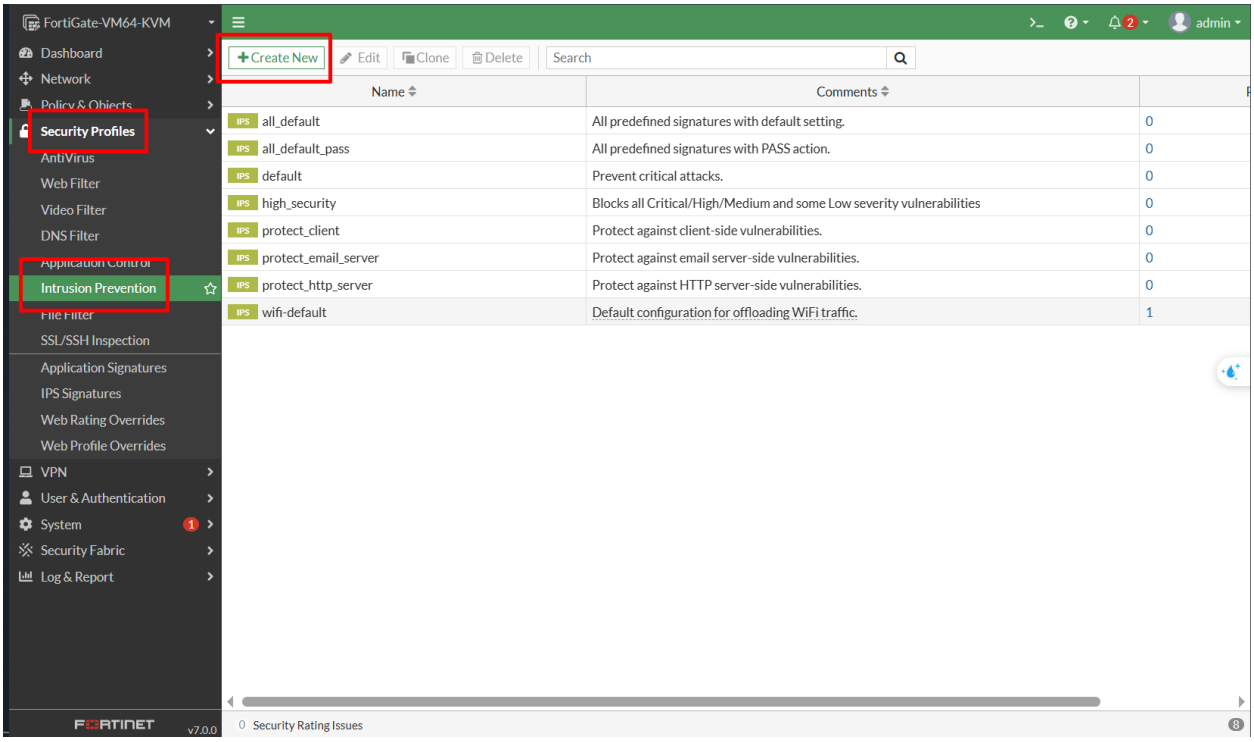
Bước 2: IPS bảo vệ hệ thống khỏi các tấn công khai thác lỗ hổng phần mềm.

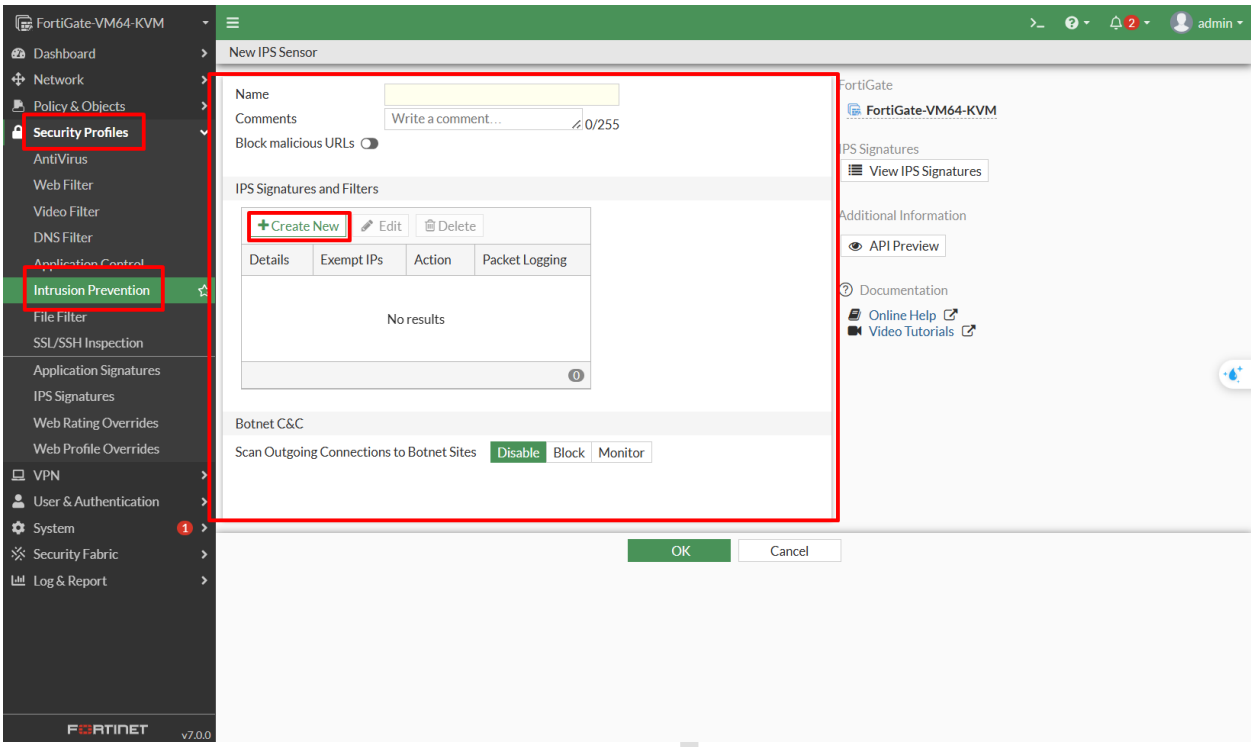
Bước 3: Chỉnh sửa profile mặc định hoặc **Create New**.

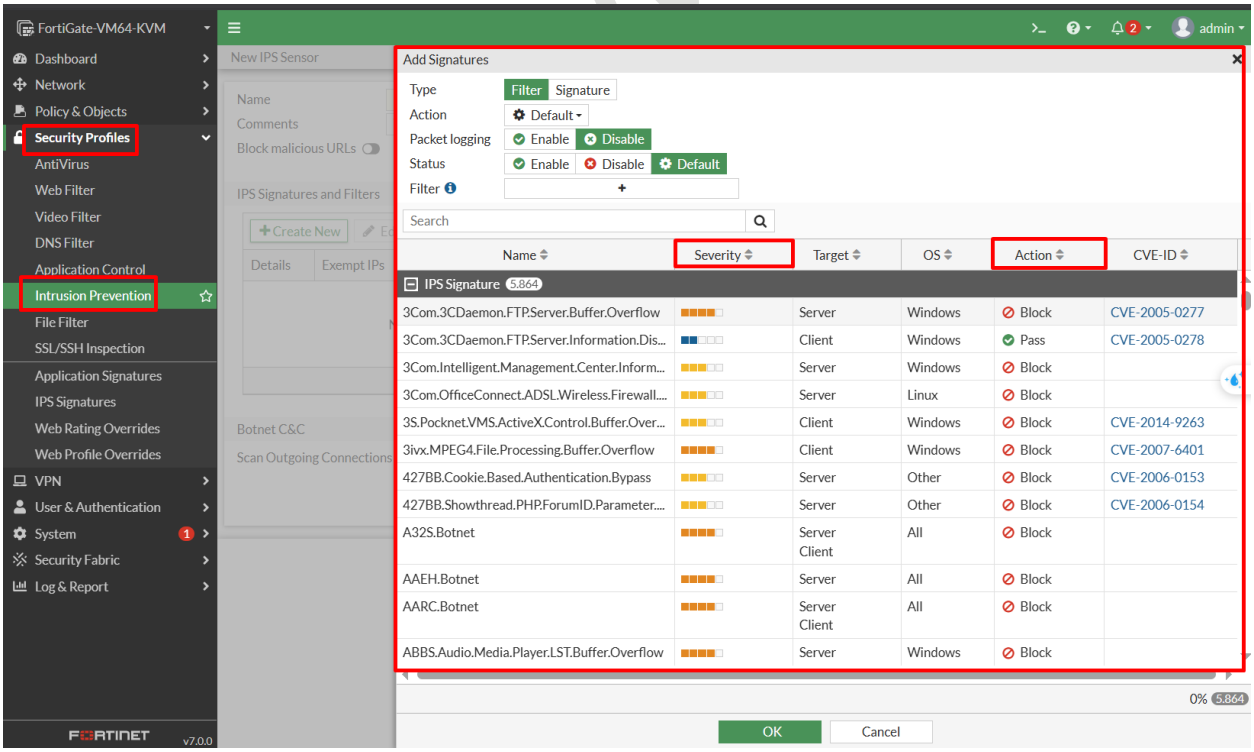
Bước 4: Trong phần **IPS Signatures and Filters**, thêm các bộ lọc với:

- – **Severity:** Critical, High, Medium
- – **Action:** Block. Hệ thống sẽ tự động chặn hàng ngàn kiểu tấn công đã nhận diện.

– Chức năng: Phát hiện và chặn các gói tin tấn công trong thời gian thực.




FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
AntiVirus
Web Filter
Video Filter
DNS Filter
Application Control
Intrusion Prevention
File Filter
SSL/SSH Inspection
Application Signatures
IPS Signatures
Web Rating Overrides
Web Profile Overrides
VPN
User & Authentication
System
Security Fabric
Log & Report
admin
New IPS Sensor
Name
Comments
Write a comment...
0/255
Block malicious URLs
IPS Signatures and Filters
Create New
Edit
Delete
Details
Exempt IPs
Action
Packet Logging
No results
Botnet C&C
Scan Outgoing Connections to Botnet Sites
Disable
Block
Monitor
FortiGate
FortiGate-VM64-KVM
IPS Signatures
View IPS Signatures
Additional Information
API Preview
Documentation
Online Help
Video Tutorials
OK
Cancel
v7.0.0


FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
AntiVirus
Web Filter
Video Filter
DNS Filter
Application Control
Intrusion Prevention
File Filter
SSL/SSH Inspection
Application Signatures
IPS Signatures
Web Rating Overrides
Web Profile Overrides
VPN
User & Authentication
System
Security Fabric
Log & Report
admin
New IPS Sensor
Add Signatures
Type
Filter
Signature
Action
Default
Packet logging
Enable
Disable
Status
Enable
Disable
Default
Filter
Search
Name
Severity
Target
OS
Action
CVE-ID
IPS Signature 5,864
3Com.3CDaemon.FTP.Server.Buffer.Overflow
Server
Windows
Block
CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Dis...
Client
Windows
Pass
CVE-2005-0278
3Com.Intelligent.Management.Center.Inform...
Server
Windows
Block
3Com.OfficeConnect.ADSL.Wireless.Firewall....
Server
Linux
Block
3S.Pocknet.VMS.ActiveX.Control.Buffer.Over...
Client
Windows
Block
CVE-2014-9263
3ivx.MPEG4.File.Processing.Buffer.Overflow
Client
Windows
Block
CVE-2007-6401
427BB.Cookie.Based.Authentication.Bypass
Server
Other
Block
CVE-2006-0153
427BB.Showthread.PHP.ForumID.Parameter....
Server
Other
Block
CVE-2006-0154
A32S.Botnet
Server
Client
All
Block
AAEH.Botnet
Server
All
Block
AARC.Botnet
Server
Client
All
Block
ABBS.Audio.Media.Player.LST.Buffer.Overflow
Server
Windows
Block
0%
5,864
OK
Cancel
v7.0.0

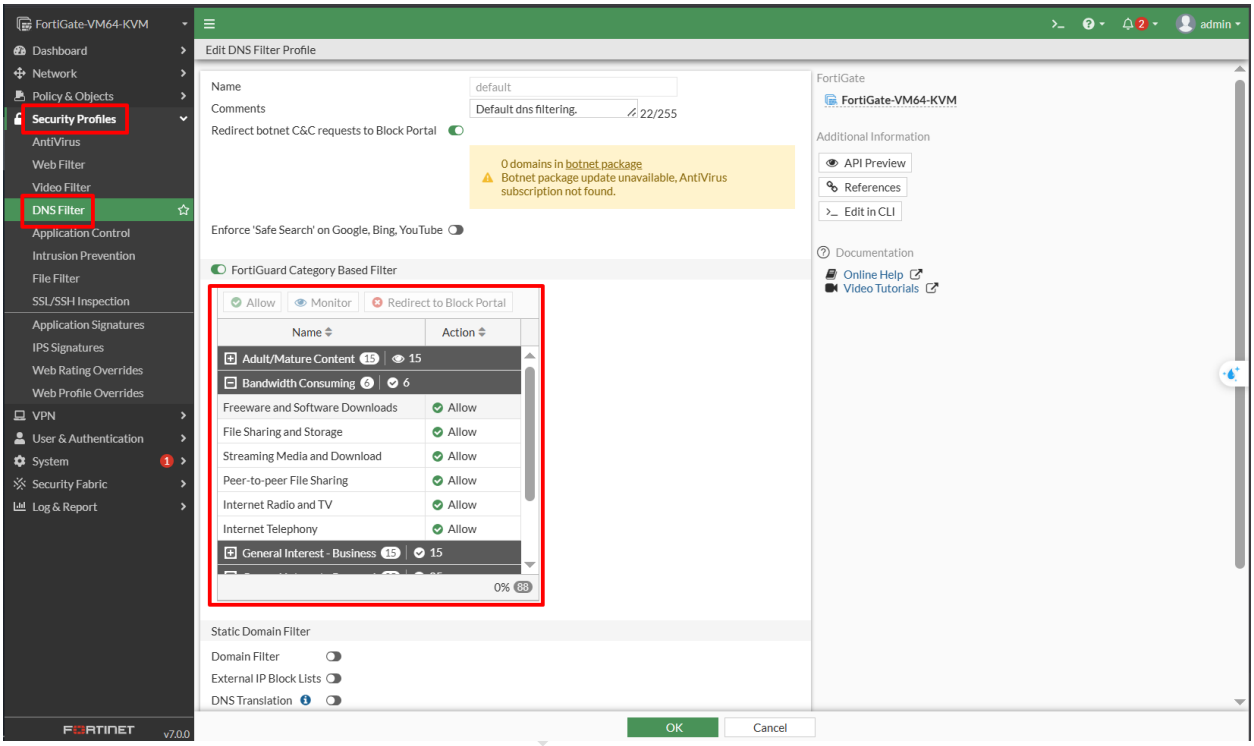
DNS Filter

Bước 1: Vào **Security Profiles > DNS Filter**.

Bước 2: Tính năng này chặn truy vấn DNS đến domain độc hại hoặc không mong muốn, trước khi kết nối TCP được tạo.

Bước 3: Bật chặn cho nhóm **Malicious Websites** và các danh mục phù hợp khác.

– Chức năng: Ngăn chặn người dùng truy cập website nguy hiểm ngay từ tầng DNS.



Tóm tắt nhanh

Profile	Mục đích chính	Ví dụ sử dụng
Antivirus	Quét virus, mã độc	Quét file HTTP, email
Web Filter	Chặn website theo danh mục	Block video, web độc hại
App Control	Kiểm soát ứng dụng	Chặn BitTorrent, game
IPS	Ngăn tấn công khai thác	Block critical/high threats
DNS Filter	Chặn domain xấu ở tầng DNS	Block malicious domains

Lưu ý sau cấu hình

Mẹo nhỏ: Sau khi tạo xong các profile, chúng ta cần **gắn** chúng vào **Firewall Policy** tương ứng để kích hoạt bảo vệ hệ thống. Việc này đảm bảo các thiết lập bảo mật được áp dụng hiệu quả trên luồng dữ liệu thực tế.

6. VPN và Kết nối bảo mật

VPN (Virtual Private Network – Mạng riêng ảo) là giải pháp bảo mật kết nối qua Internet, giúp mở rộng phạm vi truy cập an toàn giữa các điểm mạng. Chương này hướng dẫn cấu hình chi tiết SSL-VPN (Remote Access) và IPsec VPN (Site-to-Site) trên FortiGate, đồng thời chuẩn hóa thuật ngữ chuyên ngành và trình bày mạch lạc theo hướng dẫn kỹ thuật chính thống.

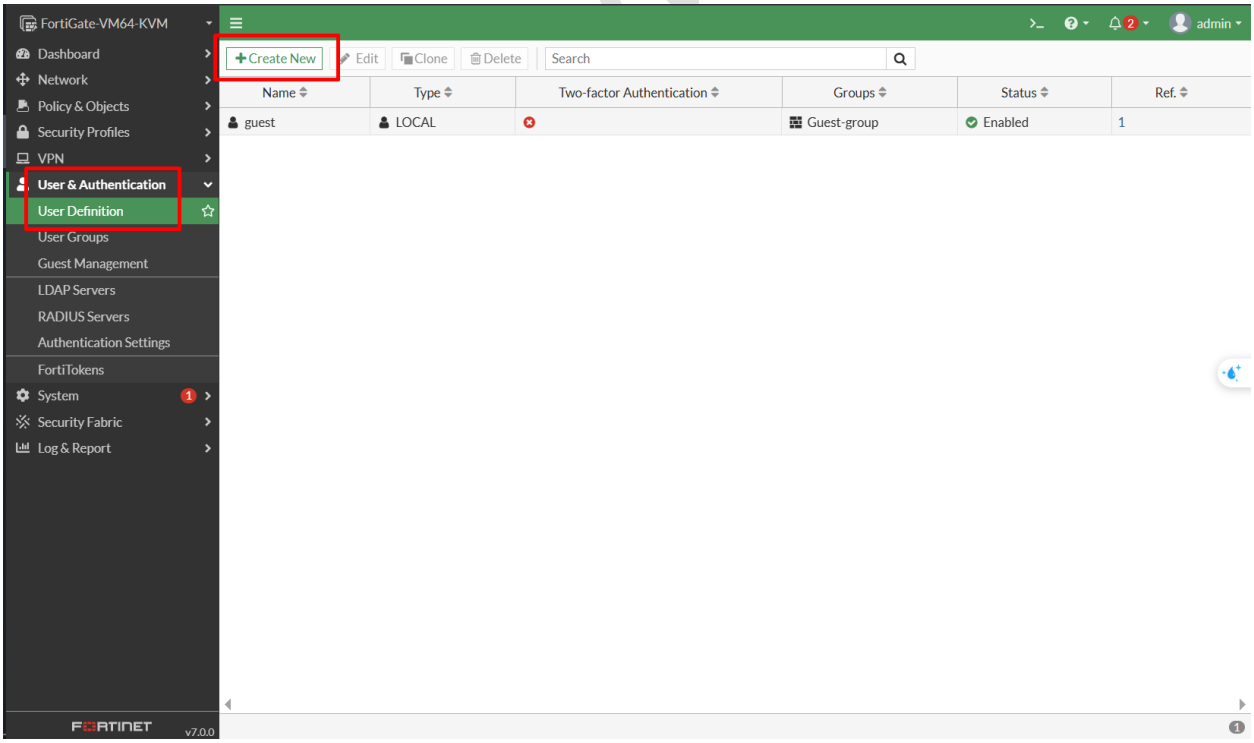
6.1 Cấu hình SSL-VPN (Remote Access)

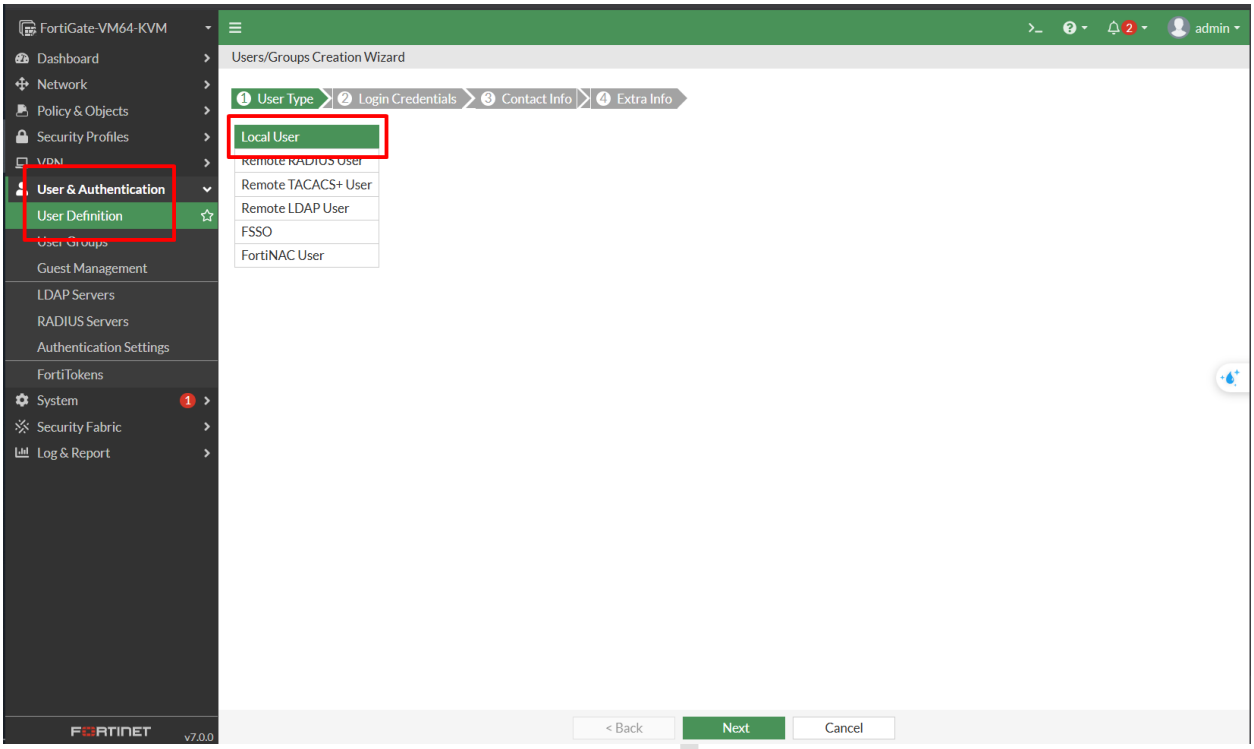
Tình huống thực tế: Đội ngũ kinh doanh thường xuyên đi công tác cần kết nối bảo mật vào mạng nội bộ văn phòng để truy cập máy chủ lưu trữ file. SSL-VPN giúp đảm bảo kết nối an toàn, mã hóa dữ liệu khi truy cập từ xa.

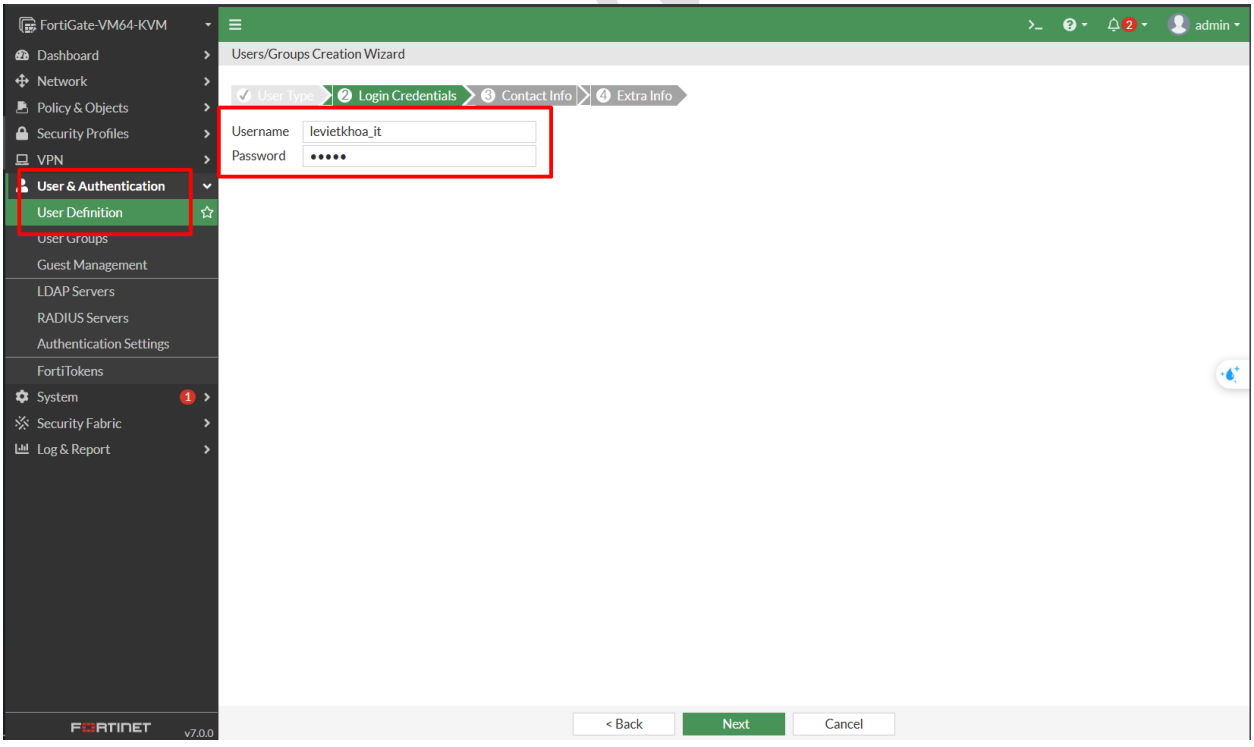
Các bước thực hiện

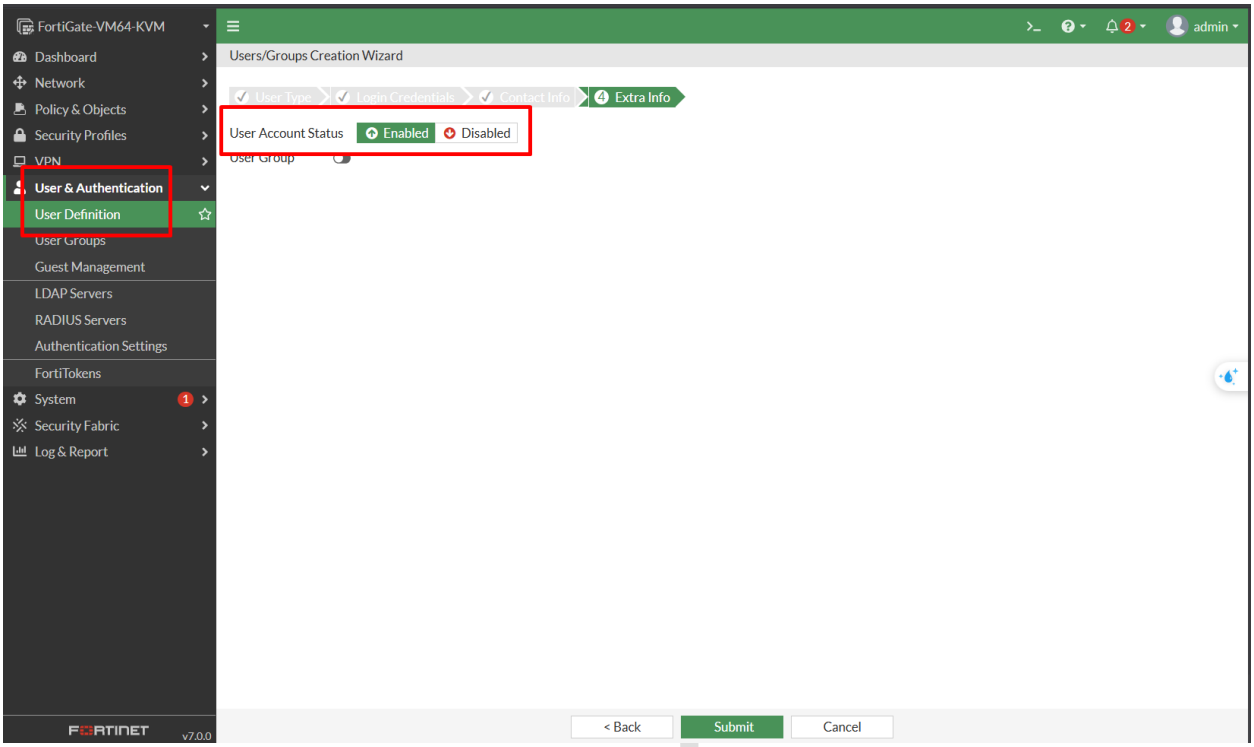
Bước 1: Tạo người dùng và nhóm người dùng

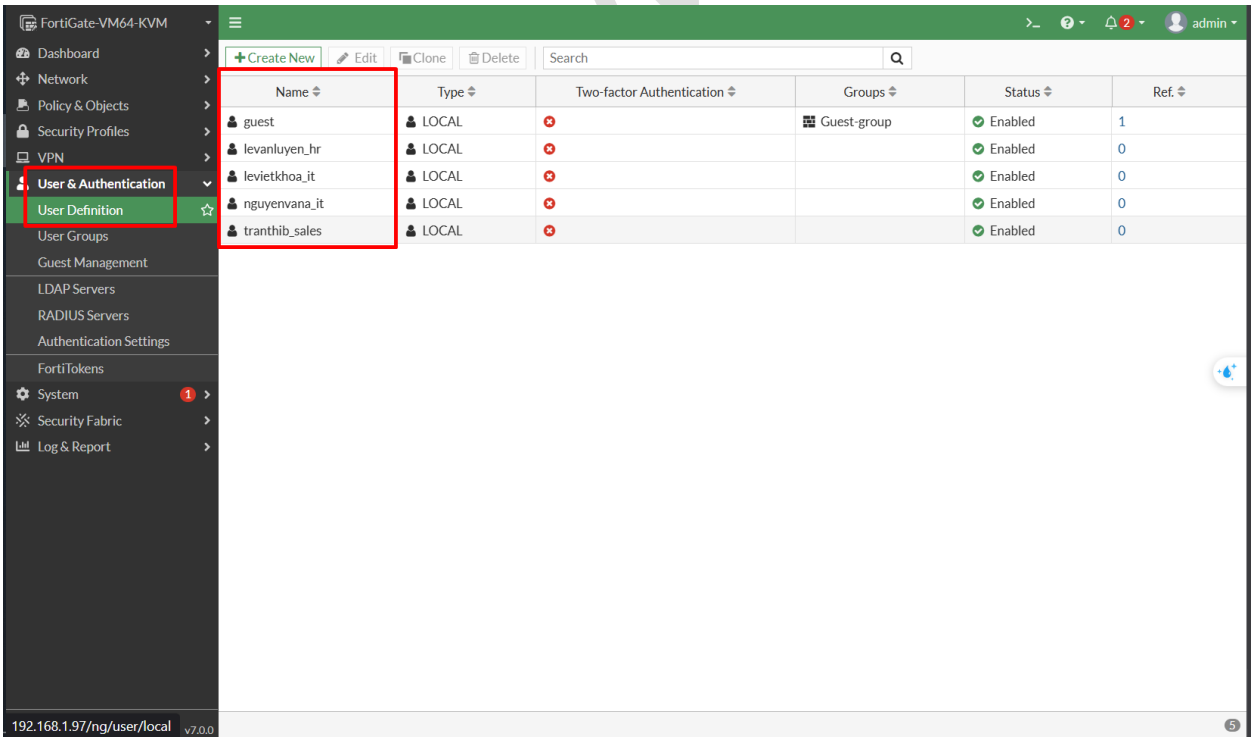
- – Truy cập **User & Authentication > User Definition** để tạo tài khoản cho từng thành viên nhóm kinh doanh.
- – Truy cập **User & Authentication > User Groups**, tạo nhóm **IT_VPN_REMOTE_ACCESS_GROUP** và thêm user vào nhóm này.

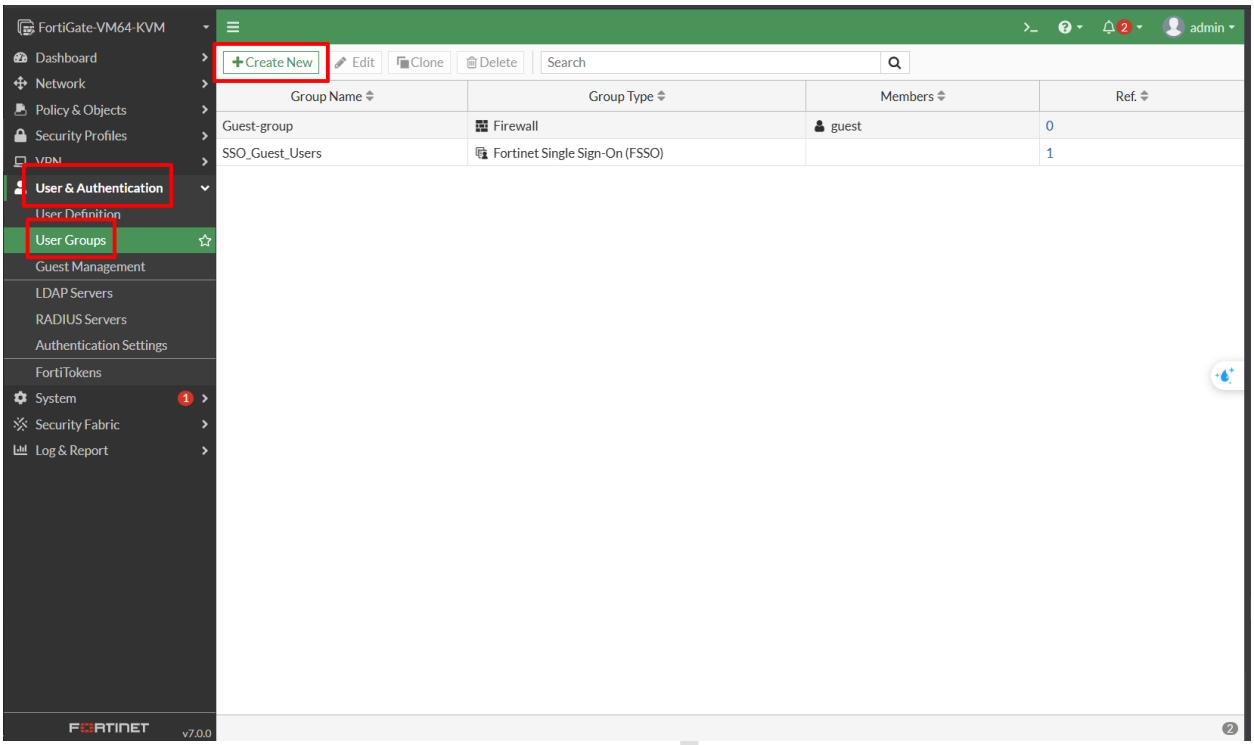


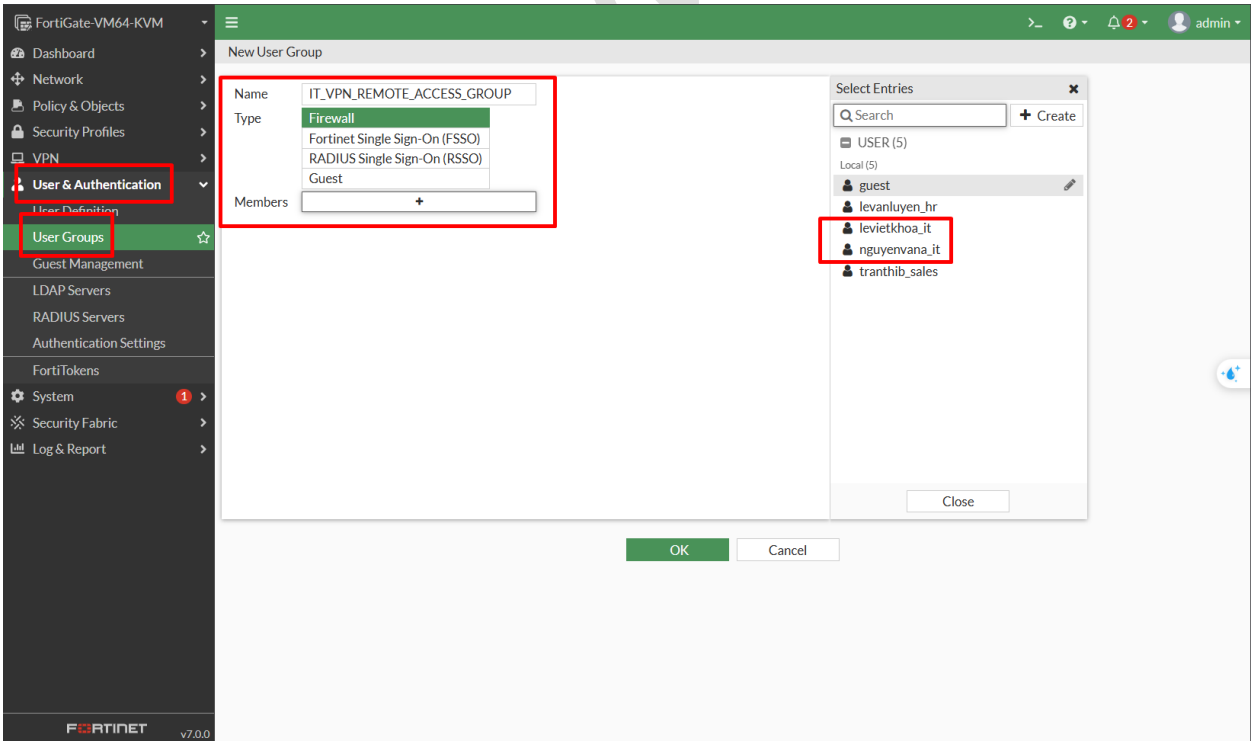

FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
System
Security Fabric
Log & Report
admin
Users/Groups Creation Wizard
1 User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Local User
Remote RADIUS User
Remote TACACS+ User
Remote LDAP User
FSSO
FortiNAC User
< Back
Next
Cancel
v7.0.0


FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
System
Security Fabric
Log & Report
admin
Users/Groups Creation Wizard
User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Username levietkhoa_it
Password
< Back
Next
Cancel
v7.0.0


FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
System
Security Fabric
Log & Report
admin
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
Extra Info
User Account Status
Enabled
Disabled
User Group
< Back
Submit
Cancel
FORTINET
v7.0.0

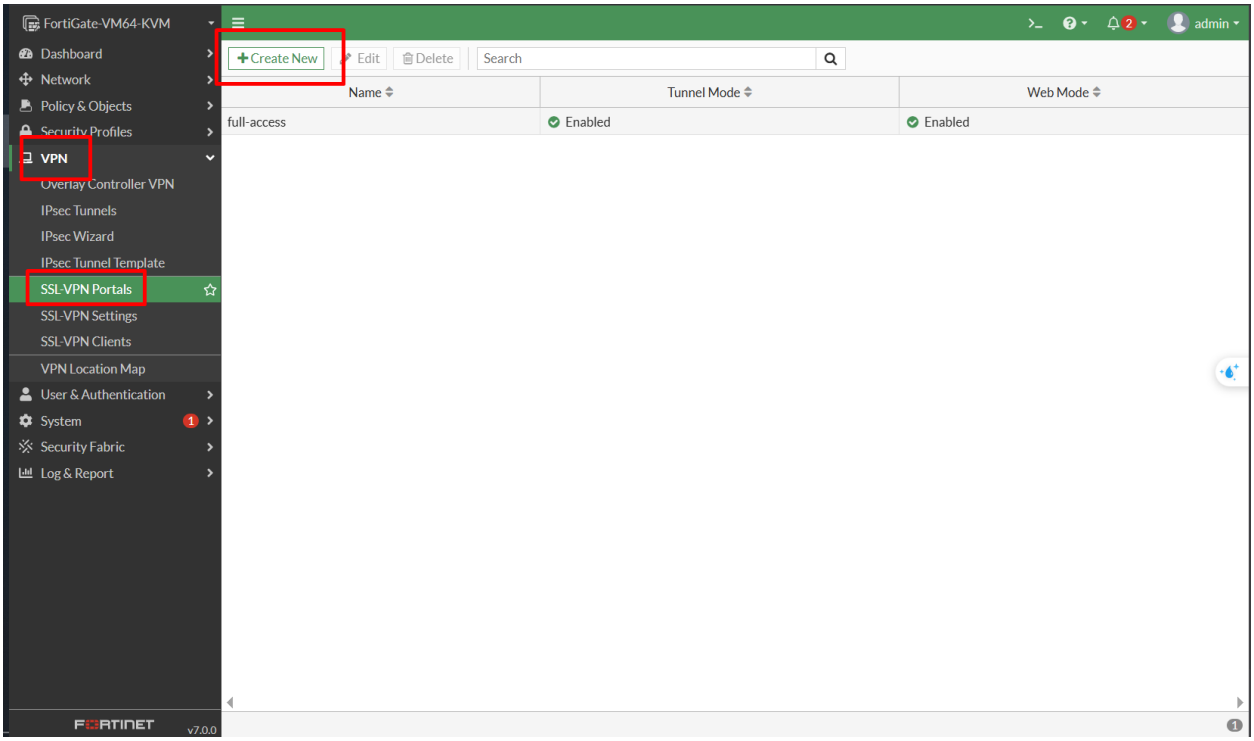

FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
System
Security Fabric
Log & Report
admin
Create New
Edit
Clone
Delete
Search
Name
Type
Two-factor Authentication
Groups
Status
Ref.
guest
LOCAL
Guest-group
Enabled
1
levanluyen_hr
LOCAL
Enabled
0
levietkhoa_it
LOCAL
Enabled
0
nguyenvana_it
LOCAL
Enabled
0
tranthib_sales
LOCAL
Enabled
0
192.168.1.97/ng/user/local
v7.0.0


FortiGate-VM64-KVM
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
System
Security Fabric
Log & Report
+ Create New
Edit
Clone
Delete
Search
Group Name
Group Type
Members
Ref.
Guest-group
Firewall
guest
0
SSO_Guest_Users
Fortinet Single Sign-On (FSSO)
1
FORTINET
v7.0.0


FortiGate-VM64-KVM
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
System
Security Fabric
Log & Report
New User Group
Name
IT_VPN_REMOTE_ACCESS_GROUP
Type
Firewall
Fortinet Single Sign-On (FSSO)
RADIUS Single Sign-On (RSSO)
Guest
Members
Select Entries
Search
Create
USER (5)
Local (5)
guest
levanluyen_hr
levietkhoa_it
nguyenvana_it
tranthib_sales
Close
OK
Cancel
FORTINET
v7.0.0

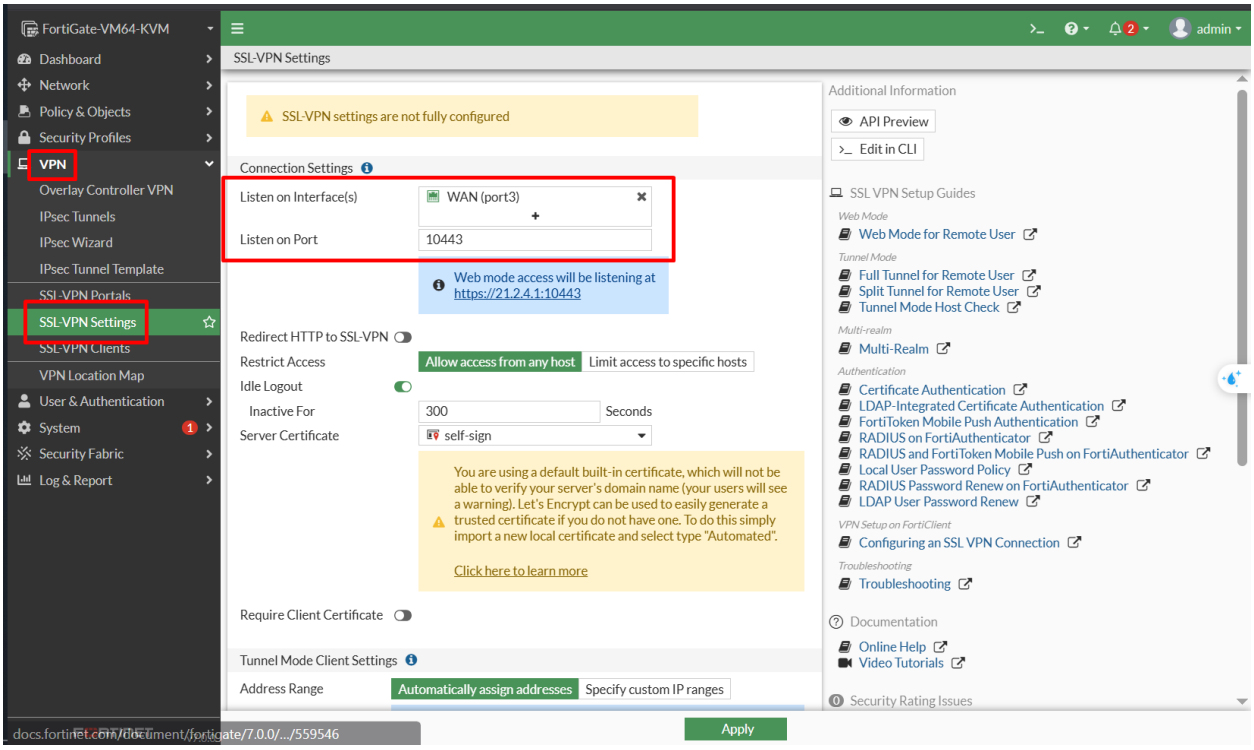
Bước 2: Cấu hình SSL-VPN Portal

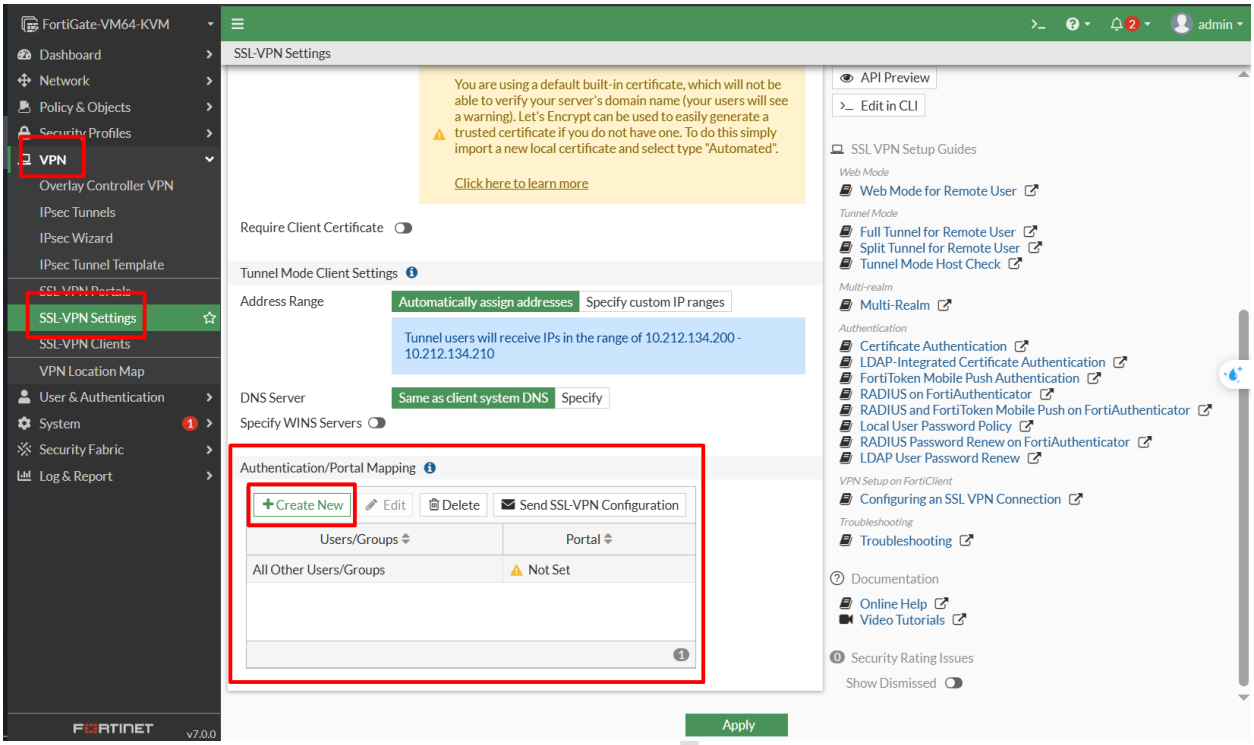
- – Truy cập **VPN > SSL-VPN Portals**. *Portal* xác định phạm vi truy cập của người dùng sau khi đăng nhập SSL-VPN.
- – Chỉnh sửa portal **full-access** sẵn có hoặc tạo mới nếu cần.
- – Đảm bảo **Tunnel Mode** được bật, cho phép người dùng truy cập toàn bộ mạng nội bộ qua VPN.

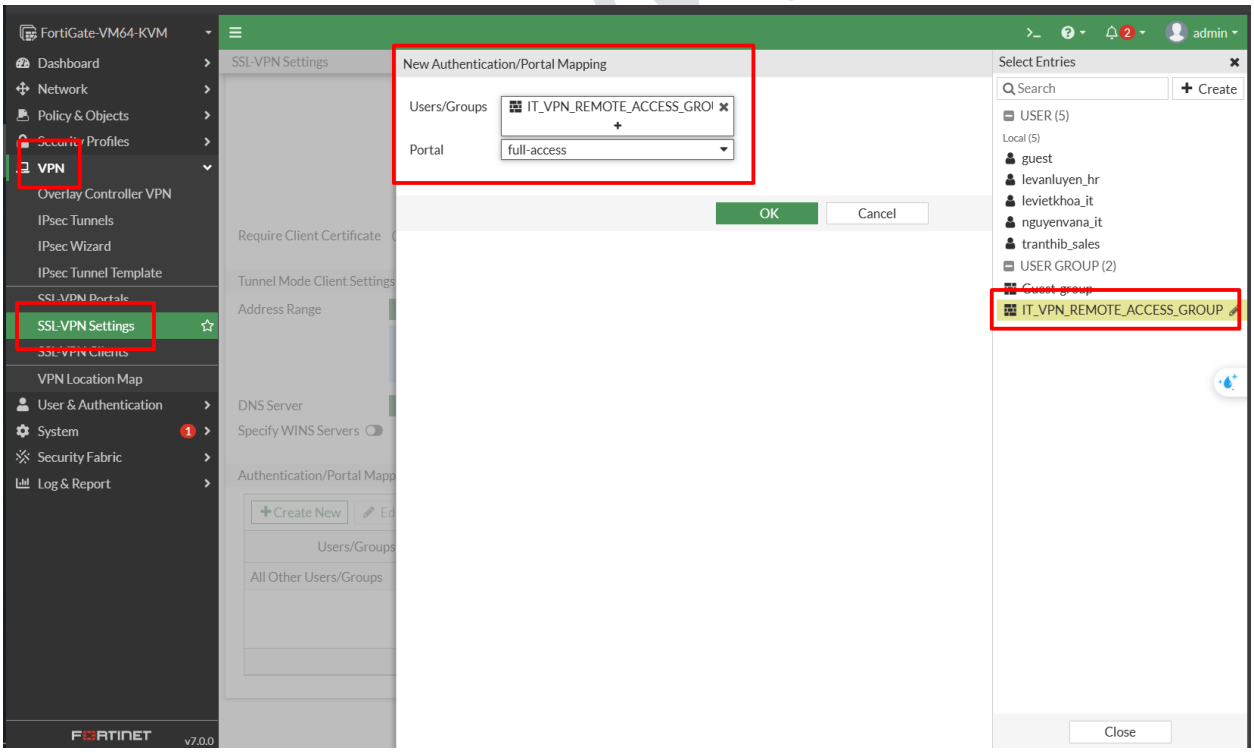


Bước 3: Cấu hình SSL-VPN Settings

- – Truy cập **VPN > SSL-VPN Settings**.
- – **Listen on Interface(s):** Chọn giao diện **WAN** (ví dụ: wan1).
- – **Listen on Port:** Cổng mặc định **443**, có thể đổi thành **10443** nếu bị chiếm dụng.
- – Trong **Authentication/Portal Mapping**, nhấn **Create New**:
  - – **User Group:** Chọn **Sales_VPN_Group**.
  - – **Portal:** Chọn **full-access**.
  - – Nhấn **OK** để lưu cấu hình



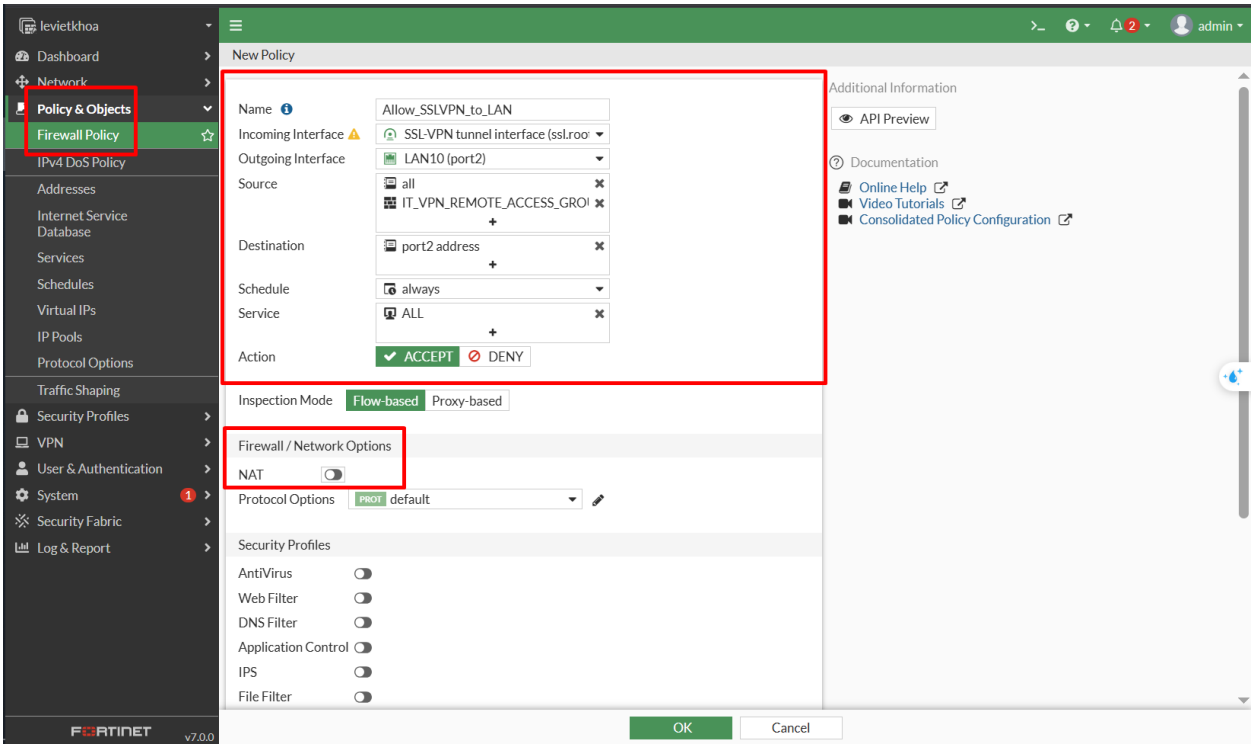

FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Settings
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
admin
SSL-VPN Settings
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one. To do this simply import a new local certificate and select type "Automated".
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Authentication/Portal Mapping
Create New
Edit
Delete
Send SSL-VPN Configuration
Users/Groups
Portal
All Other Users/Groups
Not Set
Apply
API Preview
Edit in CLI
SSL VPN Setup Guides
Web Mode
Web Mode for Remote User
Tunnel Mode
Full Tunnel for Remote User
Split Tunnel for Remote User
Tunnel Mode Host Check
Multi-realm
Multi-Realm
Authentication
Certificate Authentication
LDAP-Integrated Certificate Authentication
FortiToken Mobile Push Authentication
RADIUS on FortiAuthenticator
RADIUS and FortiToken Mobile Push on FortiAuthenticator
Local User Password Policy
RADIUS Password Renew on FortiAuthenticator
LDAP User Password Renew
VPN Setup on FortiClient
Configuring an SSL VPN Connection
Troubleshooting
Troubleshooting
Documentation
Online Help
Video Tutorials
Security Rating Issues
Show Dismissed
FORTINET
v7.0.0


FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Settings
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
admin
SSL-VPN Settings
New Authentication/Portal Mapping
Users/Groups
IT_VPN_REMOTE_ACCESS_GRO
Portal
full-access
OK
Cancel
Select Entries
Search
Create
USER (5)
Local (5)
guest
levanluyen_hr
levietkhoa_it
nguyenvana_it
tranthib_sales
USER GROUP (2)
Guest group
IT_VPN_REMOTE_ACCESS_GROUP
Close
FORTINET
v7.0.0

.

Bước 4: Tạo Firewall Policy cho kết nối VPN

- – Truy cập **Policy & Objects > Firewall Policy → Create New**.
- – Điền thông tin:
  - – **Name:** Allow_SSLVPN_to_LAN
  - – **Incoming Interface:** ssl.root (giao diện ảo cho SSL-VPN)
  - – **Outgoing Interface:** lan (mạng nội bộ)
  - – **Source:** Chọn nhóm **Sales_VPN_Group** và đối tượng **all**
  - – **Destination:** Chọn **LAN_Network** (đại diện mạng nội bộ)
  - – **Service:** ALL (hoặc giới hạn theo dịch vụ cần thiết)
  - – **Action:** ACCEPT
  - – **NAT:** OFF



Bước 5: Kết nối từ phía người dùng

- – Người dùng tải và cài đặt **FortiClient** VPN (phiên bản miễn phí đáp ứng nhu cầu cơ bản).
- – Trong **FortiClient**, tạo kết nối mới với các thông tin:
  - – Nhập địa chỉ IP công cộng của FortiGate.
  - – Đăng nhập bằng tên người dùng và mật khẩu đã cấp.

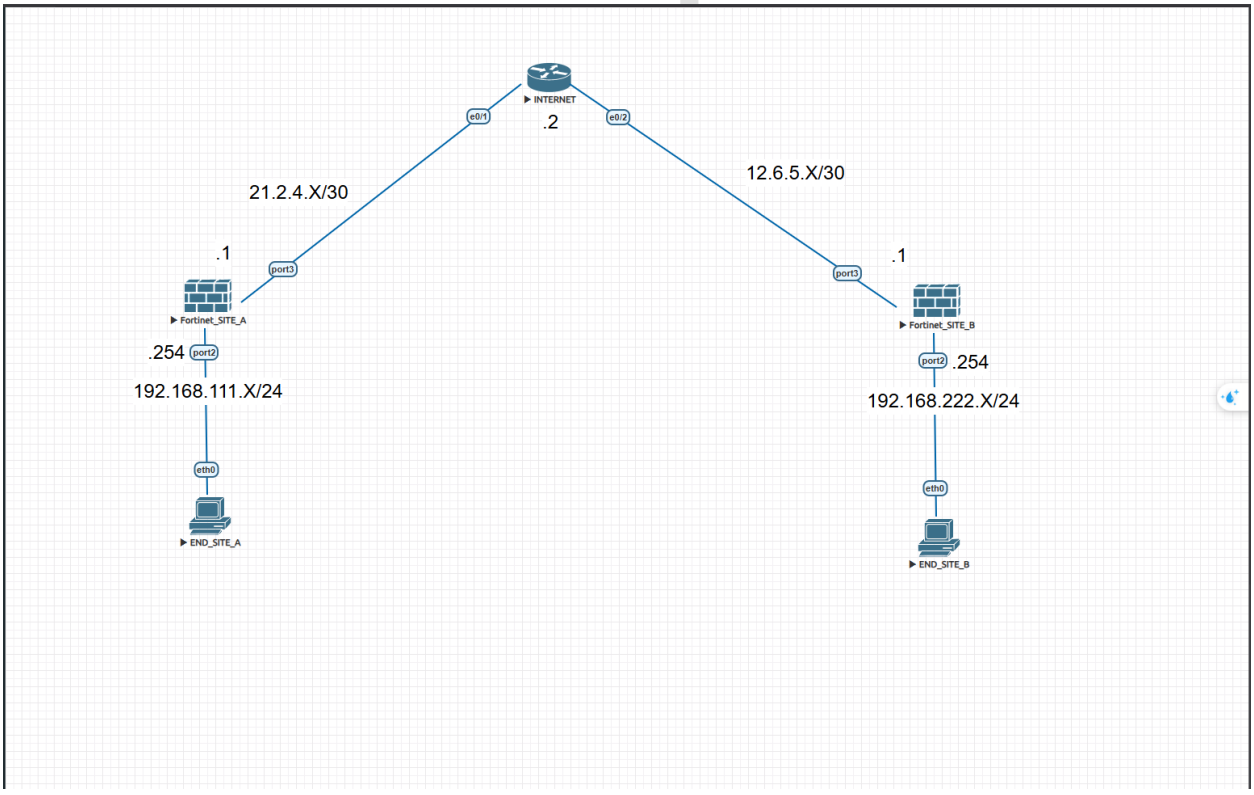
Thành phần	Vai trò
User & Group	Xác định người dùng được phép truy cập VPN
Portal	Quy định quyền truy cập sau khi kết nối
SSL-VPN Settings	Cấu hình cổng, giao diện, mapping user
Firewall Policy	Cho phép luồng SSL-VPN đến mạng LAN
FortiClient	Ứng dụng phía người dùng để kết nối VPN

Kết quả: Nhân viên có thể truy cập bảo mật vào mạng công ty từ mọi nơi qua kết nối SSL-VPN đã mã hóa.

6.2 Cấu hình IPsec VPN (Site-to-Site)

Tình huống thực tế: Thiết lập kết nối bảo mật giữa trụ sở chính (Site A) và chi nhánh (Site B) qua Internet. IPsec VPN là giải pháp hiệu quả giúp hai site truyền dữ liệu an toàn qua kênh mã hóa.

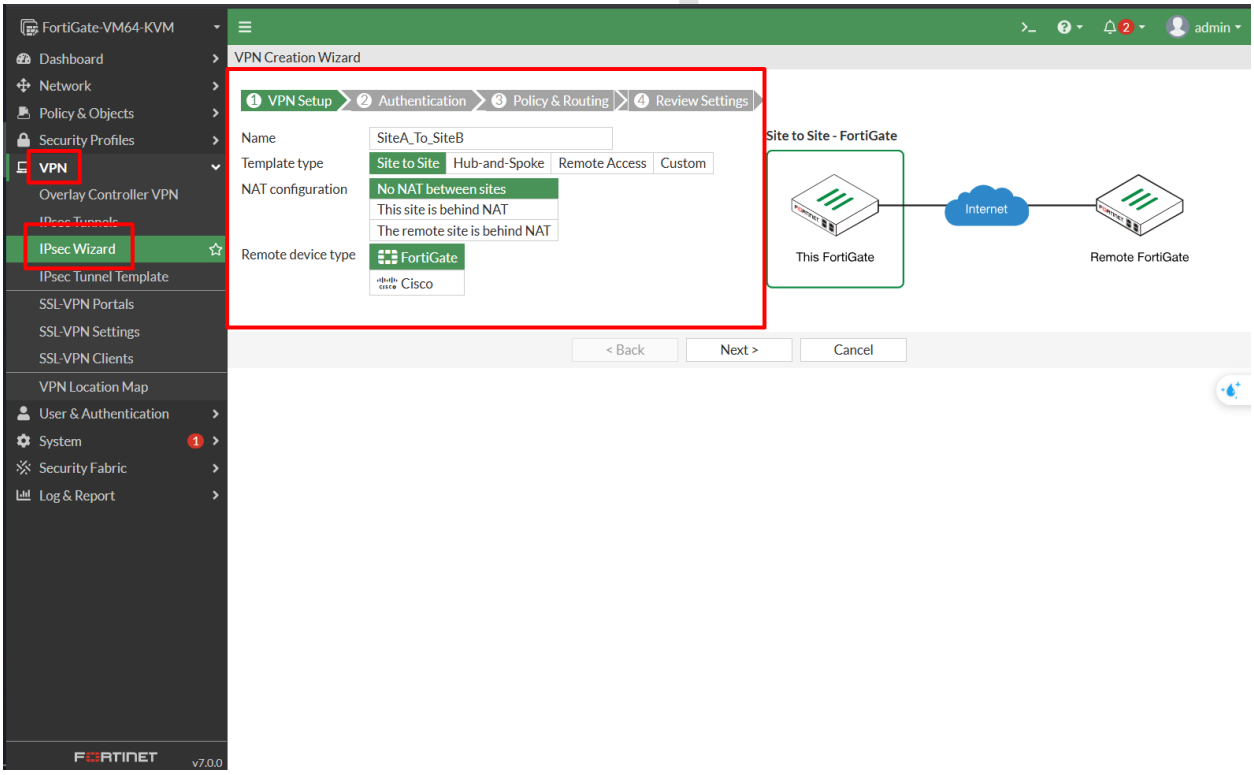
Cách đơn giản nhất để cấu hình IPsec VPN trên FortiGate là dùng **VPN Wizard**, đảm bảo thông số kỹ thuật đồng nhất ở cả hai đầu kết nối.

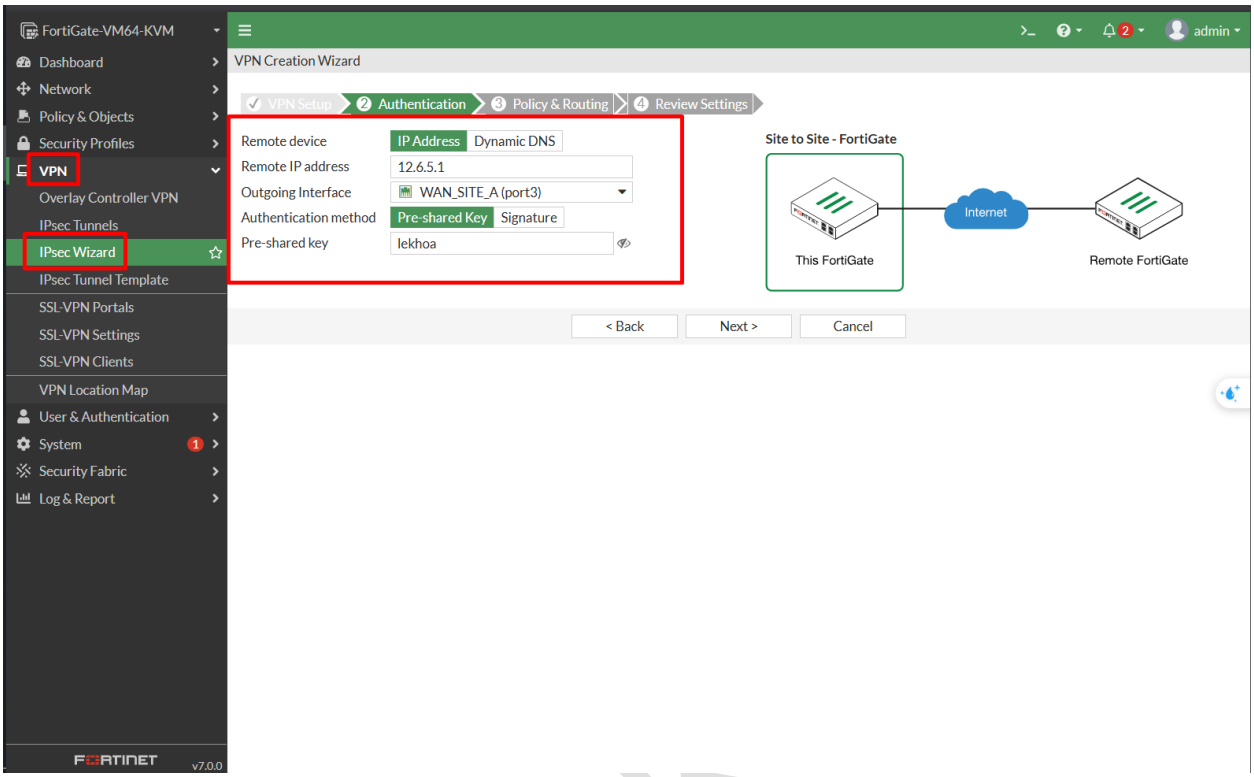


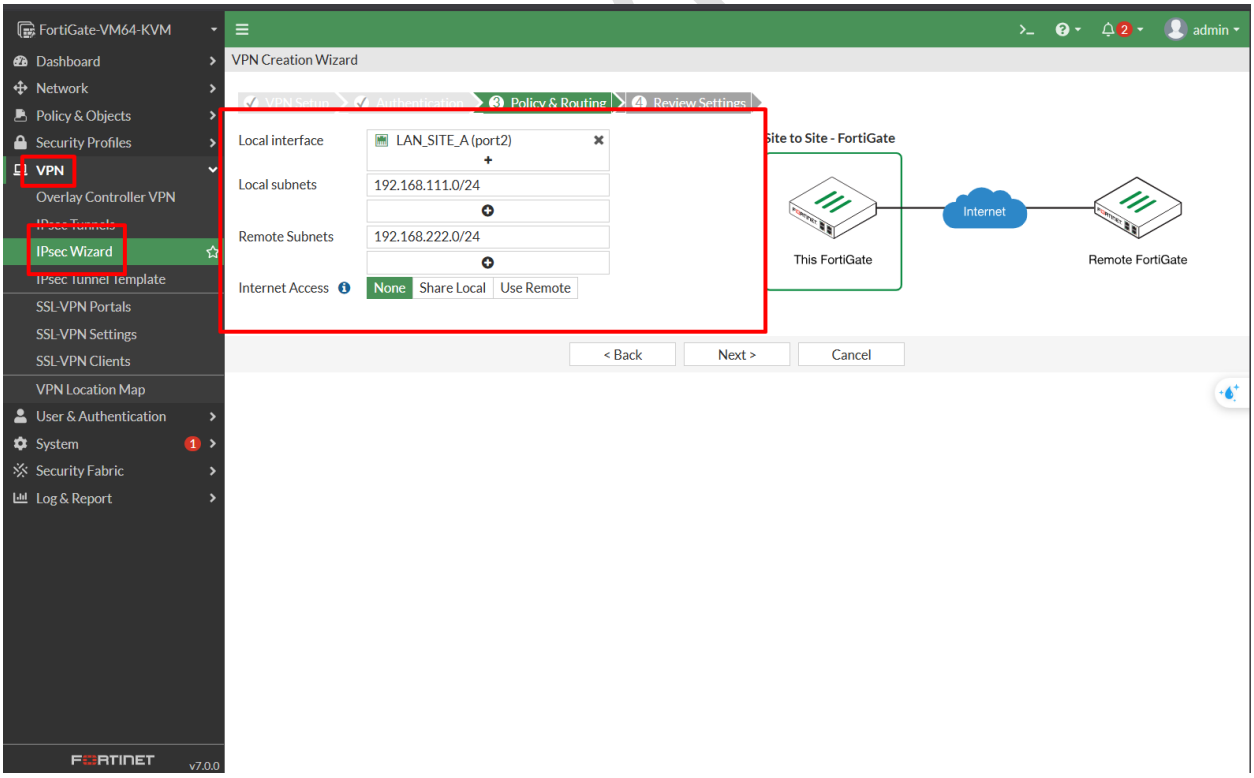
Các bước thực hiện (áp dụng cho cả hai FortiGate)

Bước 1: Tại Site A

- – Truy cập **VPN > IPsec Wizard**.
- – **Name:** to_Site_B
- – **Template Type:** Chọn *Site to Site*
- – **Remote Device Type:** Chọn *FortiGate* → nhấn **Next**
- – **Remote IP Address:** Nhập IP Public của FortiGate tại Site B
- – **Outgoing Interface:** Chọn interface kết nối Internet (ví dụ: *wan1*)
- – **Pre-shared Key:** Nhập mật khẩu mạnh (ghi lại để dùng cho Site B) → nhấn **Next**
- – **Local Interface:** Chọn interface LAN
- – **Local Subnets:** Thường được FortiGate tự động phát hiện
- – **Remote Subnets:** Nhập dải mạng LAN của Site B → nhấn **Next**
- – Kiểm tra lại tóm tắt cấu hình → nhấn **Create**




FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
admin
VPN Creation Wizard
VPN Setup
Authentication
Policy & Routing
Review Settings
Remote device
IP Address
Dynamic DNS
Remote IP address
12.6.5.1
Outgoing Interface
WAN_SITE_A (port3)
Authentication method
Pre-shared Key
Signature
Pre-shared key
lekhoa
Site to Site - FortiGate
This FortiGate
Internet
Remote FortiGate
< Back
Next >
Cancel
FORTINET
v7.0.0

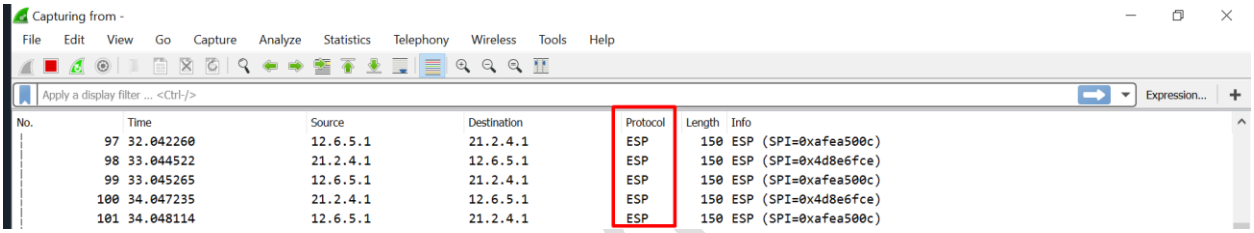

FortiGate-VM64-KVM
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
admin
VPN Creation Wizard
Policy & Routing
Review Settings
Local interface
LAN_SITE_A (port2)
Local subnets
192.168.111.0/24
Remote Subnets
192.168.222.0/24
Internet Access
None
Share Local
Use Remote
Site to Site - FortiGate
This FortiGate
Internet
Remote FortiGate
< Back
Next >
Cancel
FORTINET
v7.0.0

Bước 2: Tại Site B

- – Thực hiện tương tự, nhưng **đảo ngược** thông tin:
- – **Remote IP Address:** Nhập IP Public của Site A
- – **Pre-shared Key:** Sử dụng đúng key đã tạo bên Site A
- – **Remote Subnets:** Nhập dải mạng LAN của Site A

Sau khi hoàn thành cấu hình ở cả hai site, IPsec tunnel sẽ tự động khởi tạo. Kiểm tra trạng thái kết nối tại **Monitor > IPsec Monitor**. Nếu trạng thái hiển thị **Up** (màu xanh), hai site đã kết nối thành công. Toàn bộ lưu lượng giữa hai mạng LAN sẽ đi qua đường hầm VPN được mã hóa.

Lưu ý: Khi bắt gói tin truyền giữa hai site bằng Wireshark, dữ liệu đã được mã hóa hoàn toàn đảm bảo bảo mật thông tin.



Best Practices (Khuyến nghị cấu hình an toàn)

- – **Pre-shared Key mạnh:** Sử dụng chuỗi dài, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- – **Mã hóa và xác thực mạnh:** Ở Phase 1 và Phase 2, chọn **AES256 + SHA256** để tối ưu hóa bảo mật.
- – **Bật Dead Peer Detection (DPD):** Tính năng này giúp FortiGate tự động phát hiện khi đầu bên kia bị ngắt, tự tái kết nối nhanh chóng, duy trì tính liên tục của VPN.

7. Quản lý, Logging và Xử lý sự cố

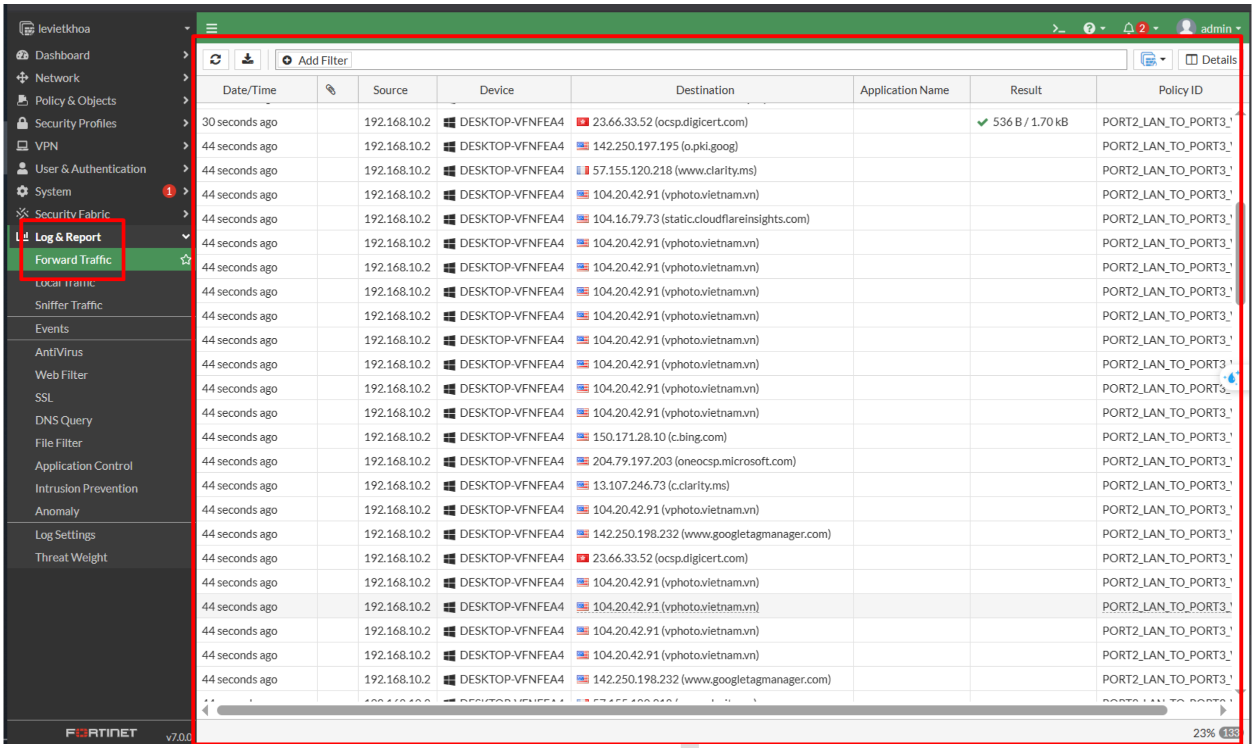
7.1 Logging và Reporting

FortiGate tạo ra lượng lớn dữ liệu log phục vụ cho công tác giám sát, phân tích và đảm bảo an ninh hệ thống. Để quản trị hiệu quả, chúng ta cần nắm rõ quy trình truy cập, phân loại và sử dụng các log này theo đúng chuẩn Fortinet.

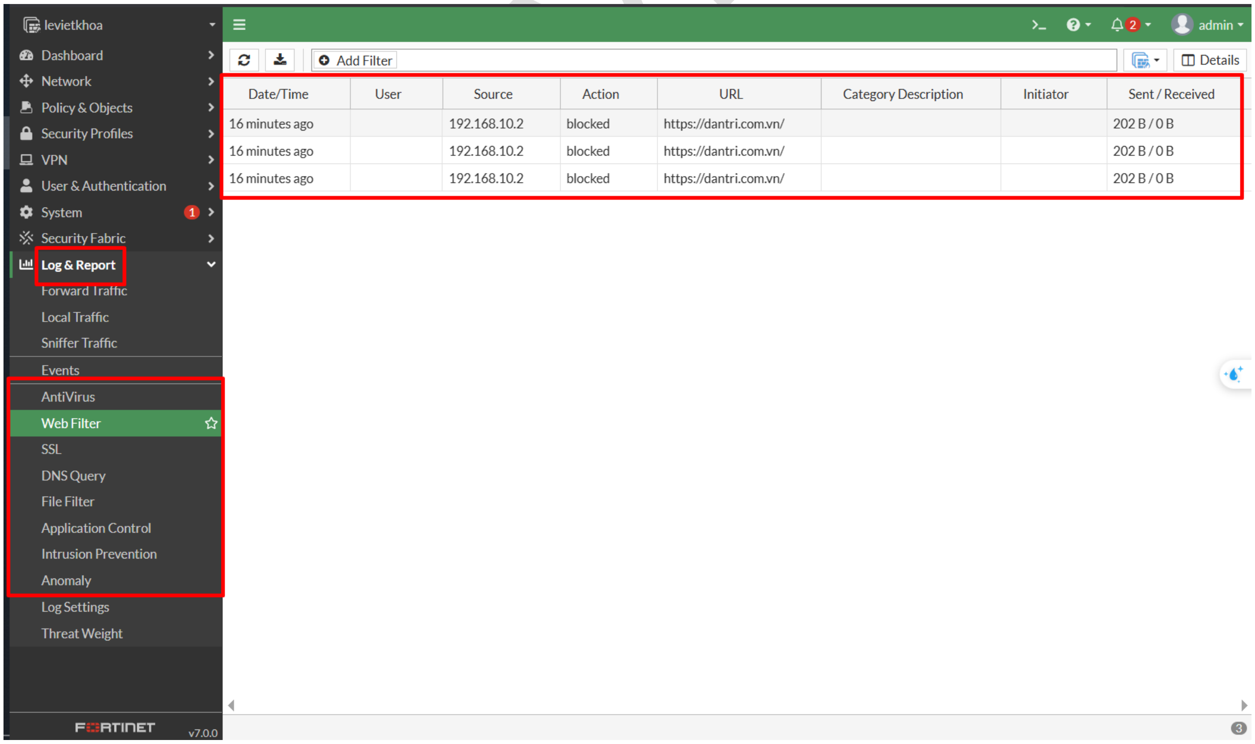
Các bước truy cập log

Bước 1: Truy cập mục **Log & Report** trên giao diện quản trị FortiGate.

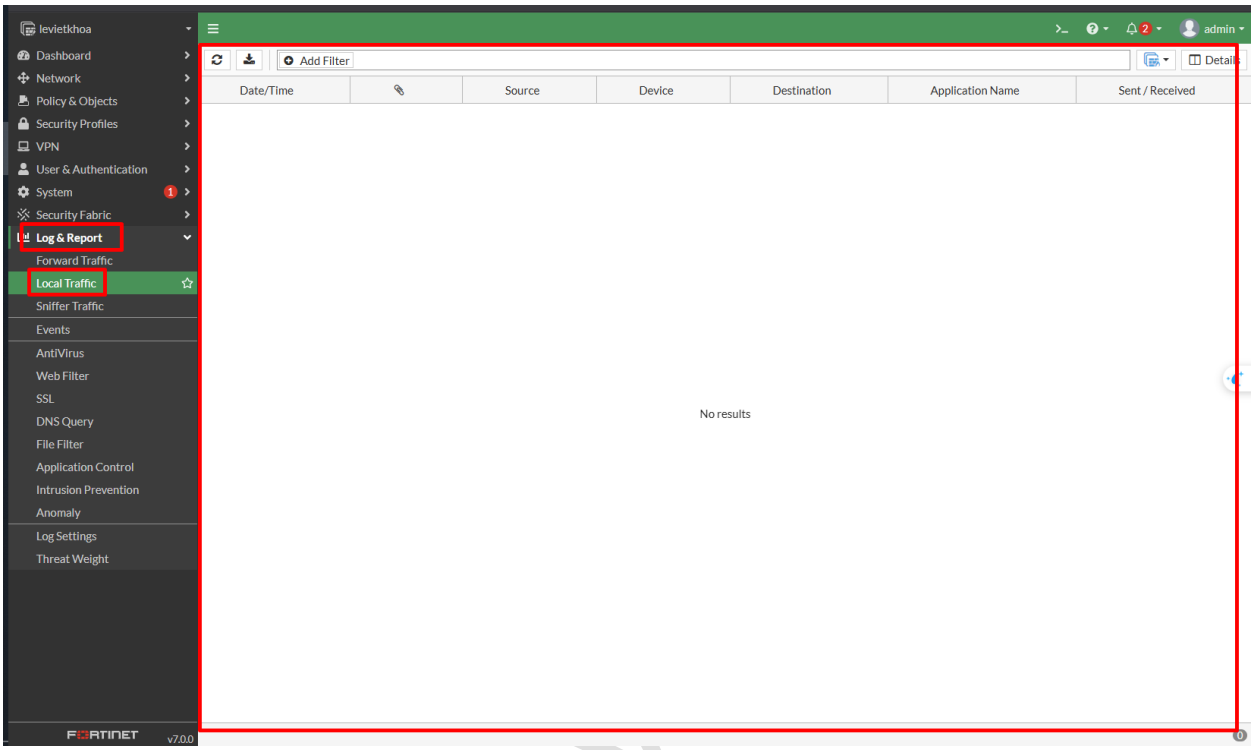
Bước 2: Kiểm tra **Forward Traffic** – đây là loại log thường xuyên sử dụng để theo dõi các phiên (session) được phép hoặc bị từ chối bởi các Firewall Policy.



Bước 3: Theo dõi **Security Events** – log ghi nhận các sự kiện từ các Security Profile như Web Filter, AntiVirus, Application Control…



Bước 4: Sử dụng **Local Reports** – FortiGate hỗ trợ tạo báo cáo cơ bản trực tiếp trên thiết bị. Chúng ta truy cập **Log & Report > Reports** để xem các báo cáo phục vụ công tác quản trị.



Ghi chú nâng cao

Khi phát sinh nhu cầu logging hoặc phân tích chuyên sâu, chúng ta nên triển khai các giải pháp sau:

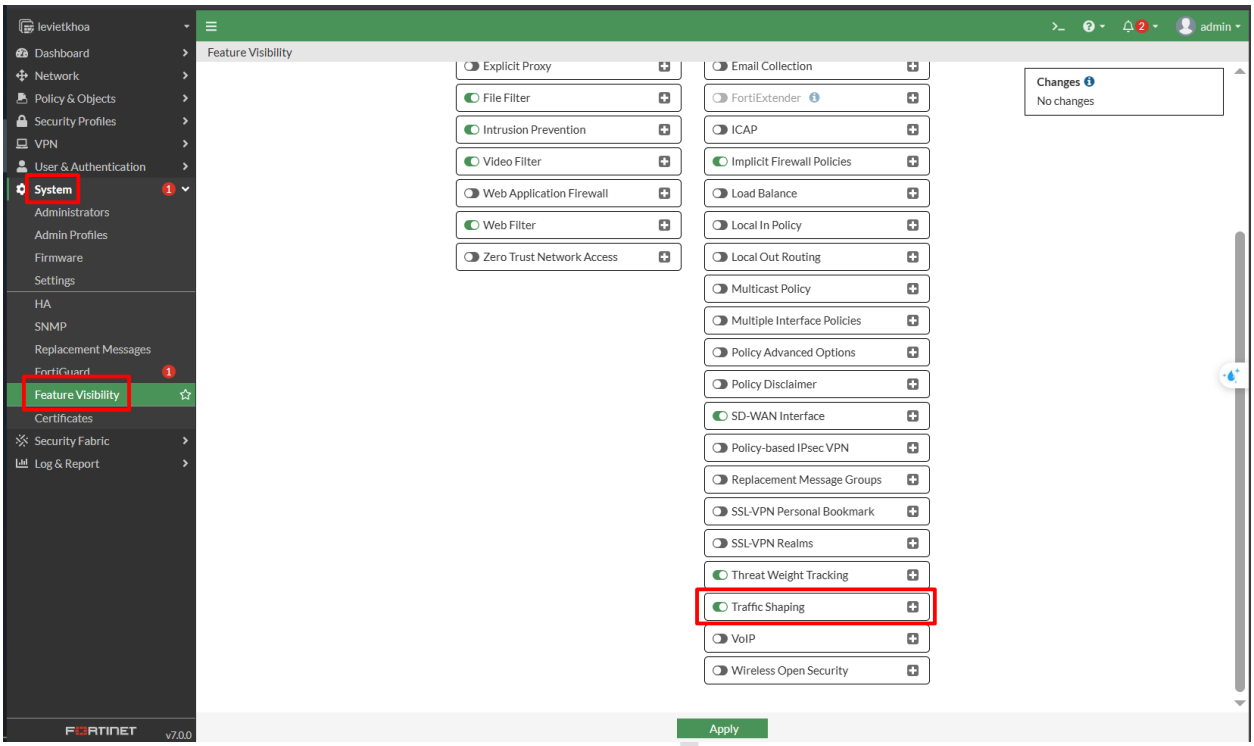
- – **FortiAnalyzer**: Thiết bị hoặc máy ảo chuyên dụng để lưu trữ, phân tích và tổng hợp log tập trung từ nhiều thiết bị FortiGate.
- – **FortiCloud**: Dịch vụ lưu trữ và phân tích log trên nền tảng đám mây, phù hợp cho việc lưu trữ log dài hạn và quản lý tập trung nhiều site.

Lưu ý kỹ thuật: Sử dụng FortiAnalyzer hoặc FortiCloud giúp nâng cao năng lực giám sát bảo mật, phát hiện sớm các mối đe dọa và tối ưu hóa quy trình báo cáo cũng như quản trị hệ thống mạng.

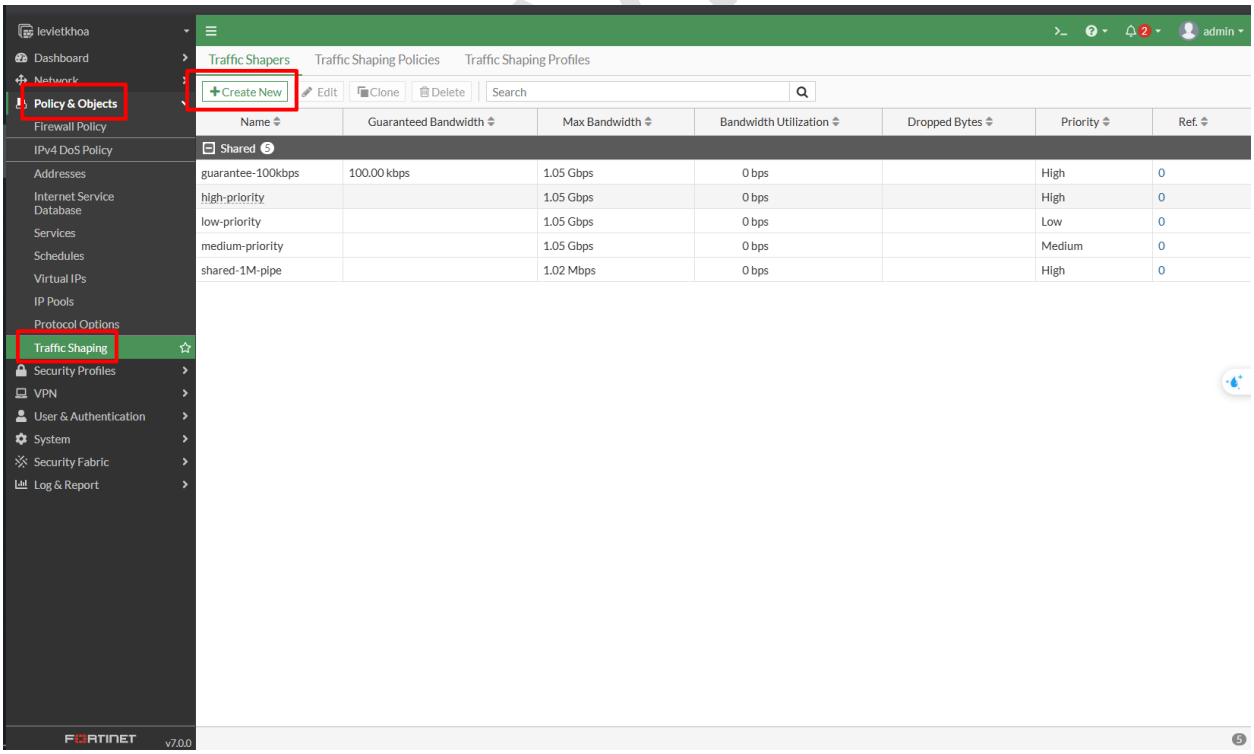
7.2 Traffic Shaping

Để kiểm soát băng thông (Bandwidth) và tối ưu tài nguyên mạng, chúng ta sử dụng tính năng Traffic Shaping trên FortiGate. Các bước cấu hình cơ bản cần tuân thủ như sau:

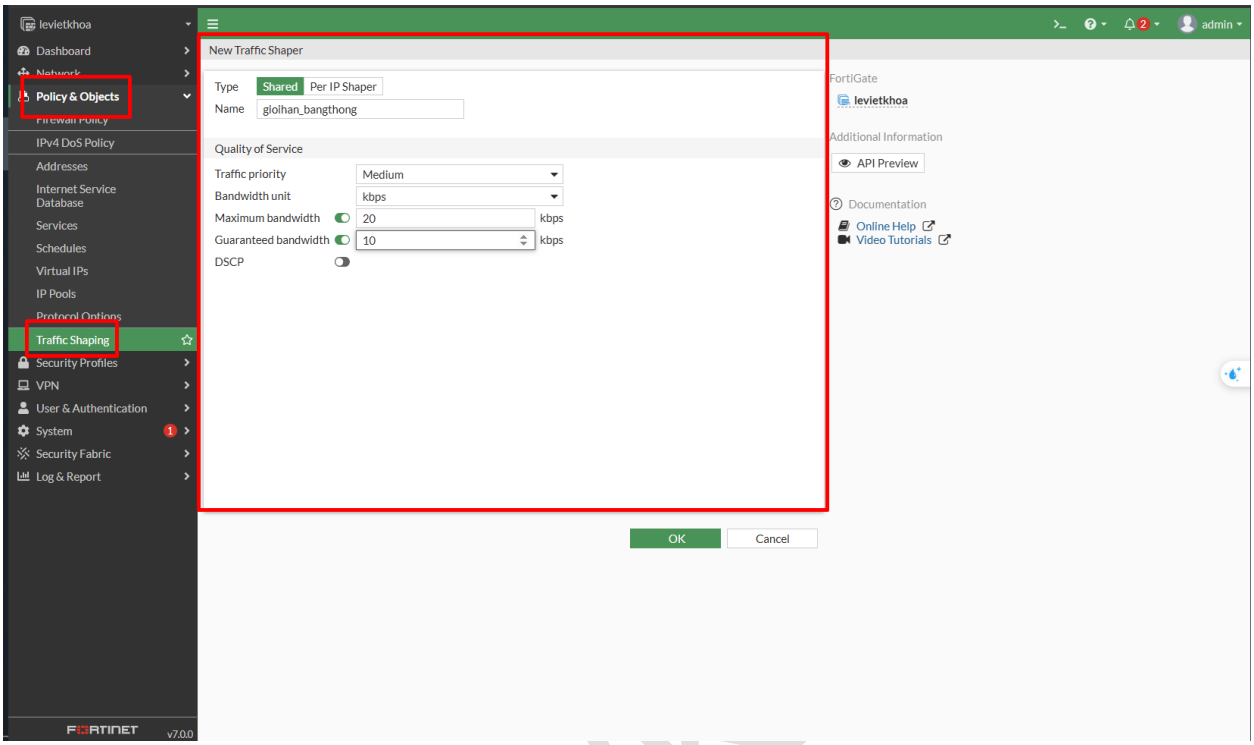
Bước 1: Truy cập **Feature Visibility** và kích hoạt tính năng Traffic Shaping.



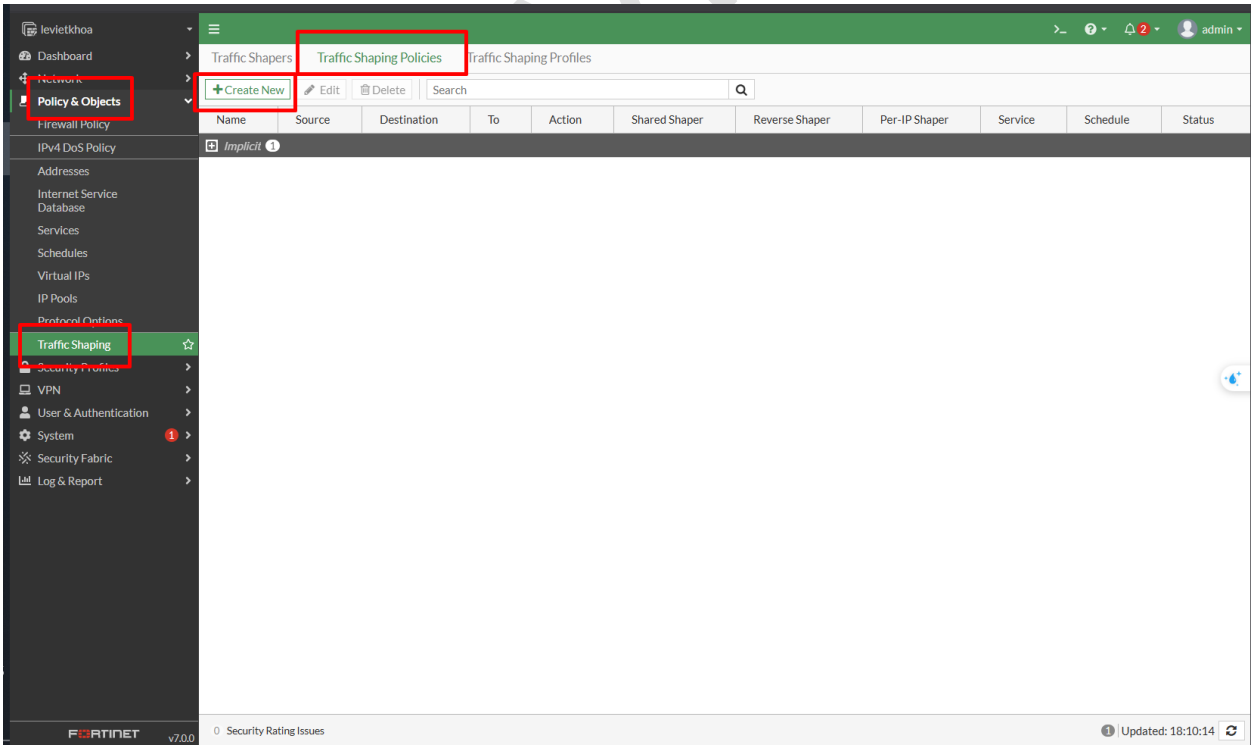
Bước 2: Vào **Policy & Objects > Traffic Shapers** để tạo mới policy quản lý băng thông, ví dụ: *gioihan_bangthong*.

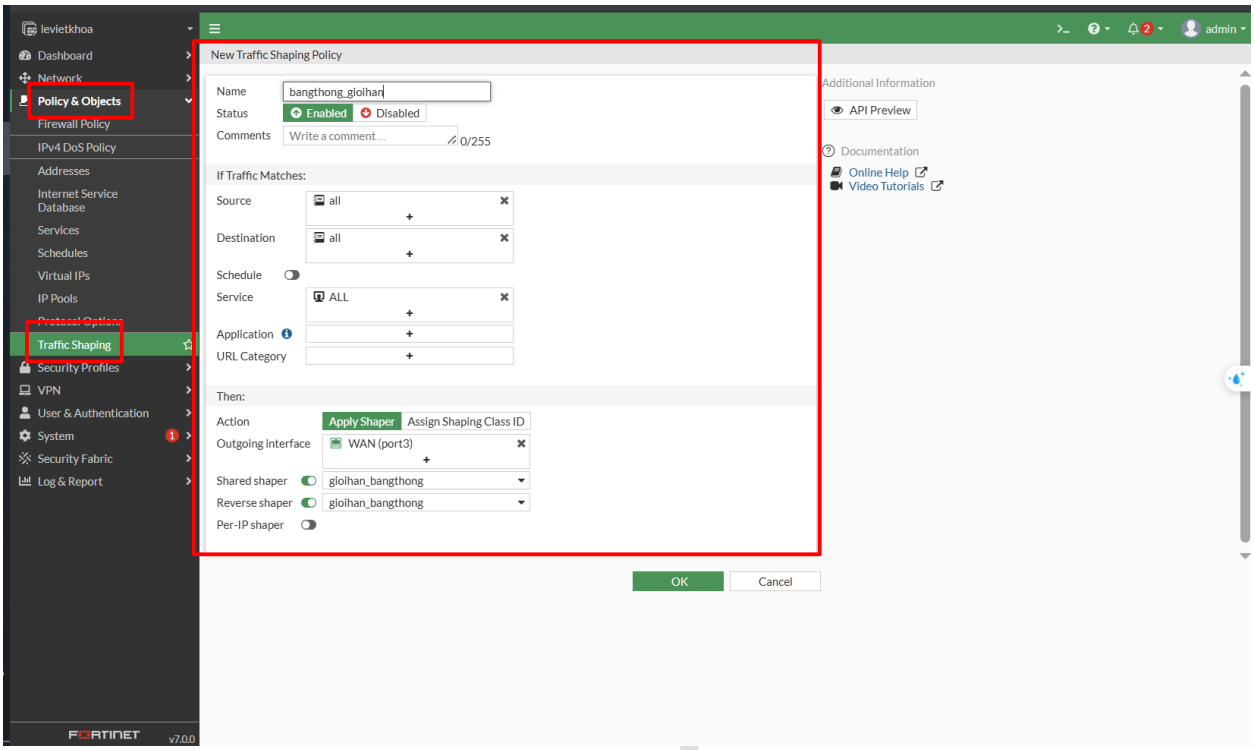


Bước 3: Thiết lập các thông số Max/Min (Guaranteed) Bandwidth, đơn vị tính là kbps.

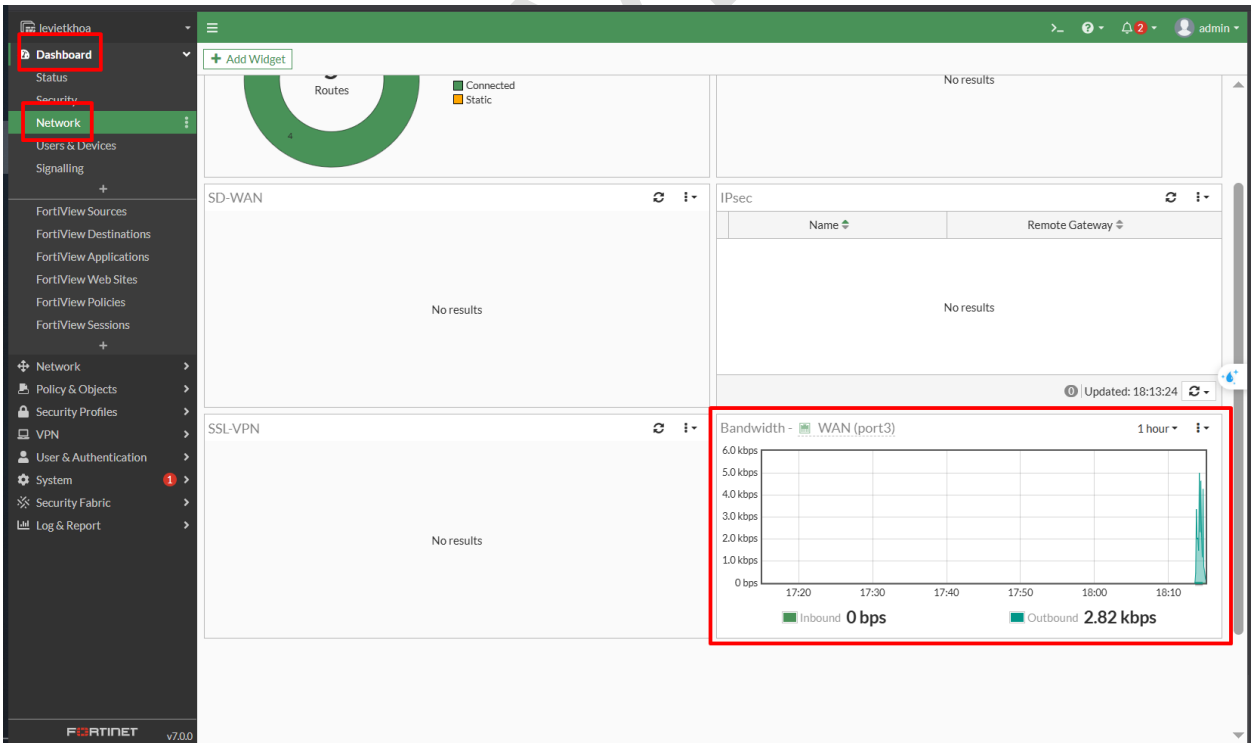


Bước 4: Gán policy vừa tạo vào interface outgoing (ví dụ: port 3).





Bước 5: Tại **Dashboard > Network**, quan sát lưu lượng in/outbound để đảm bảo không vượt quá giới hạn đã thiết lập.



7.3 Sao lưu và Khôi phục cấu hình

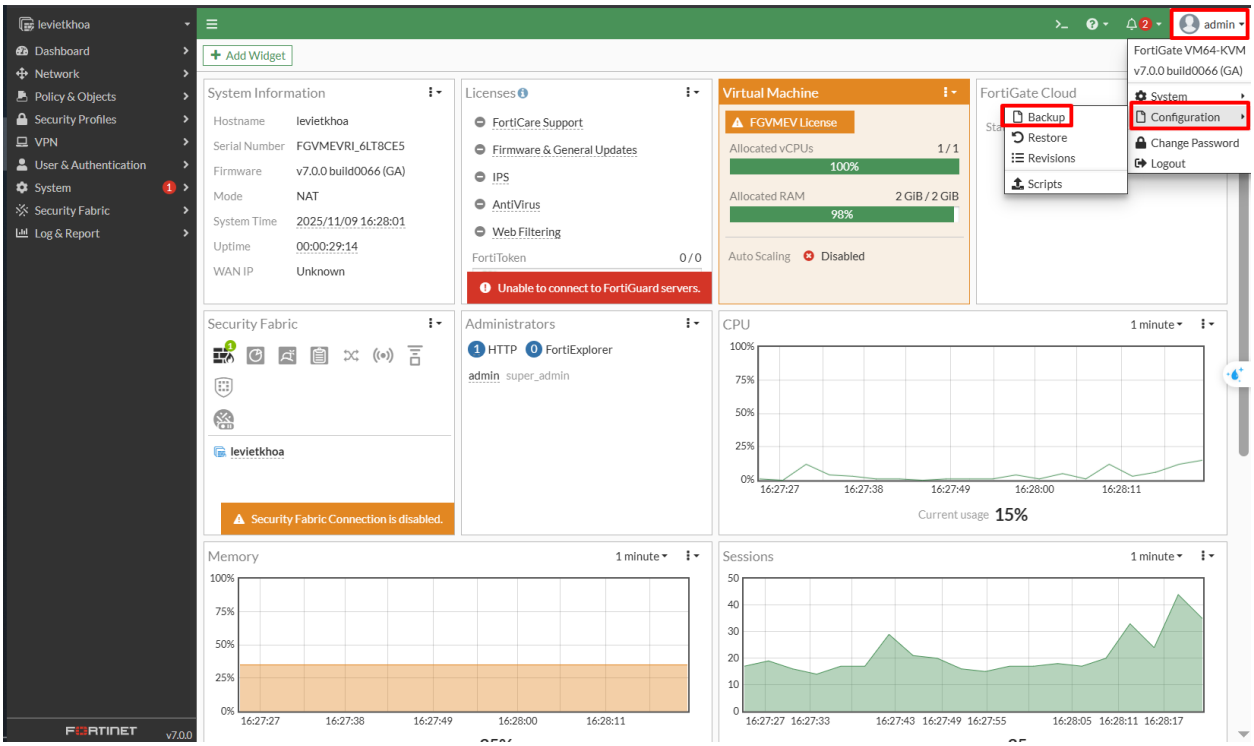
Lưu ý kỹ thuật: Chúng ta nên thực hiện sao lưu (backup) cấu hình thường xuyên, đặc biệt trước khi tiến hành thay đổi lớn hoặc nâng cấp firmware để đảm bảo an toàn dữ liệu.

Các bước sao lưu (Backup)

Bước 1: Trên giao diện FortiGate, nhấp vào tên tài khoản **Administrator** ở góc trên bên phải, chọn **Configuration > Backup**.

Bước 2: Lưu file cấu hình định dạng .conf vào vị trí an toàn ngoài thiết bị.

Bước 3: Có thể chọn mã hóa file backup bằng mật khẩu để tăng cường bảo mật.



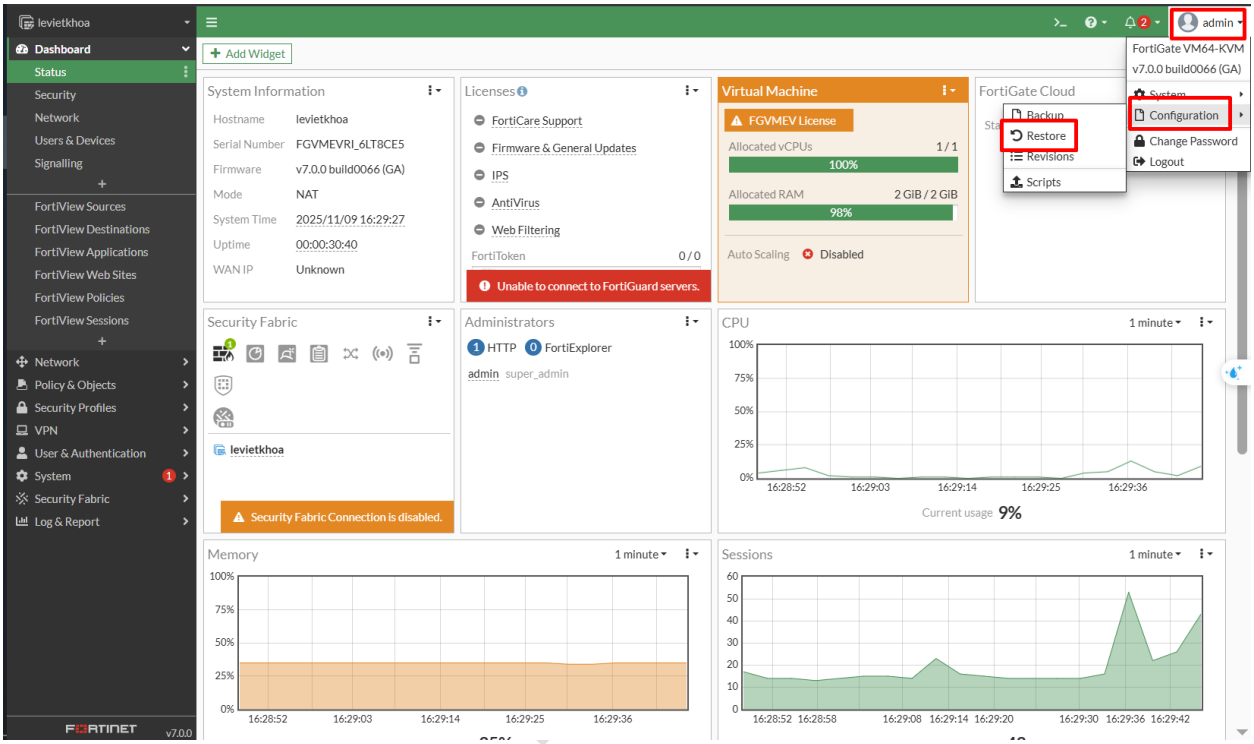
Các bước khôi phục (Restore)

Bước 1: Truy cập cùng vị trí backup, chọn **Restore**.

Bước 2: Upload file .conf đã lưu trước đó.

Bước 3: Thiết bị sẽ khởi động lại và áp dụng cấu hình đã khôi phục.

Khuyến nghị: Luôn duy trì ít nhất một bản backup cấu hình ngoài thiết bị (off-device) để phòng trường hợp sự cố hoặc lỗi phần cứng, đảm bảo khả năng phục hồi nhanh chóng.



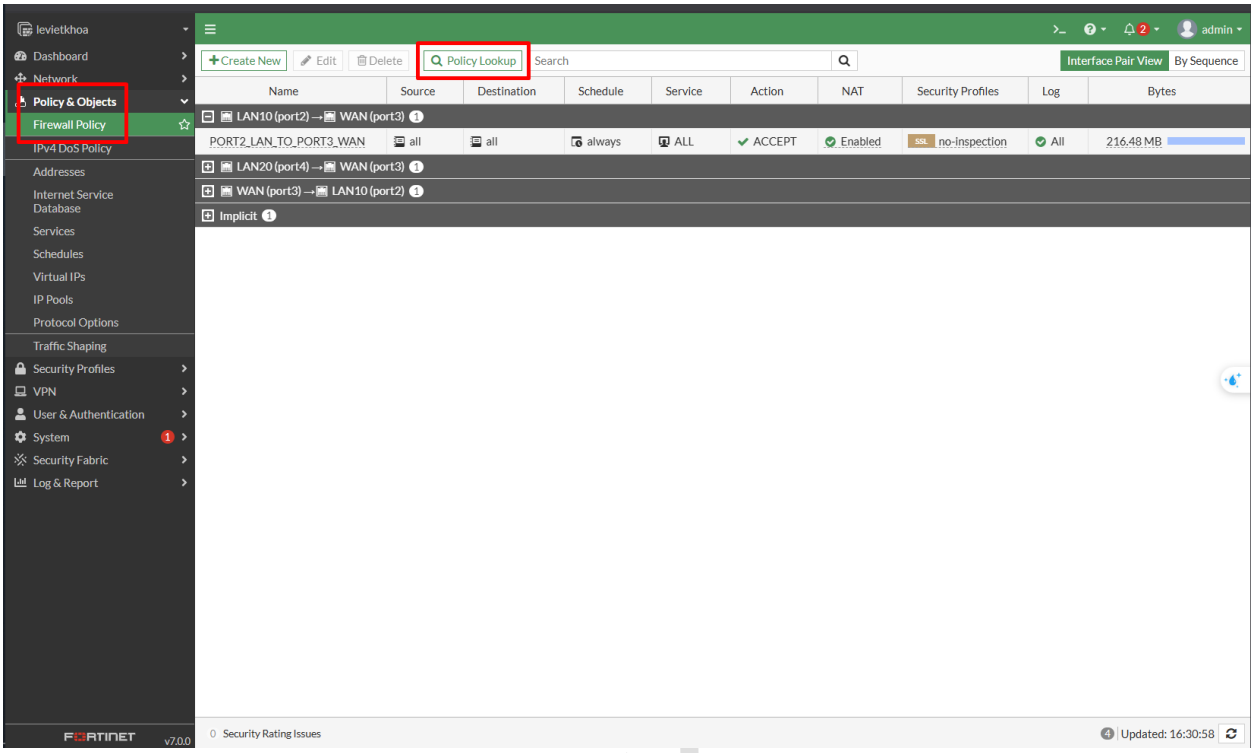
7.4 Xử lý sự cố cơ bản (Basic Troubleshooting)

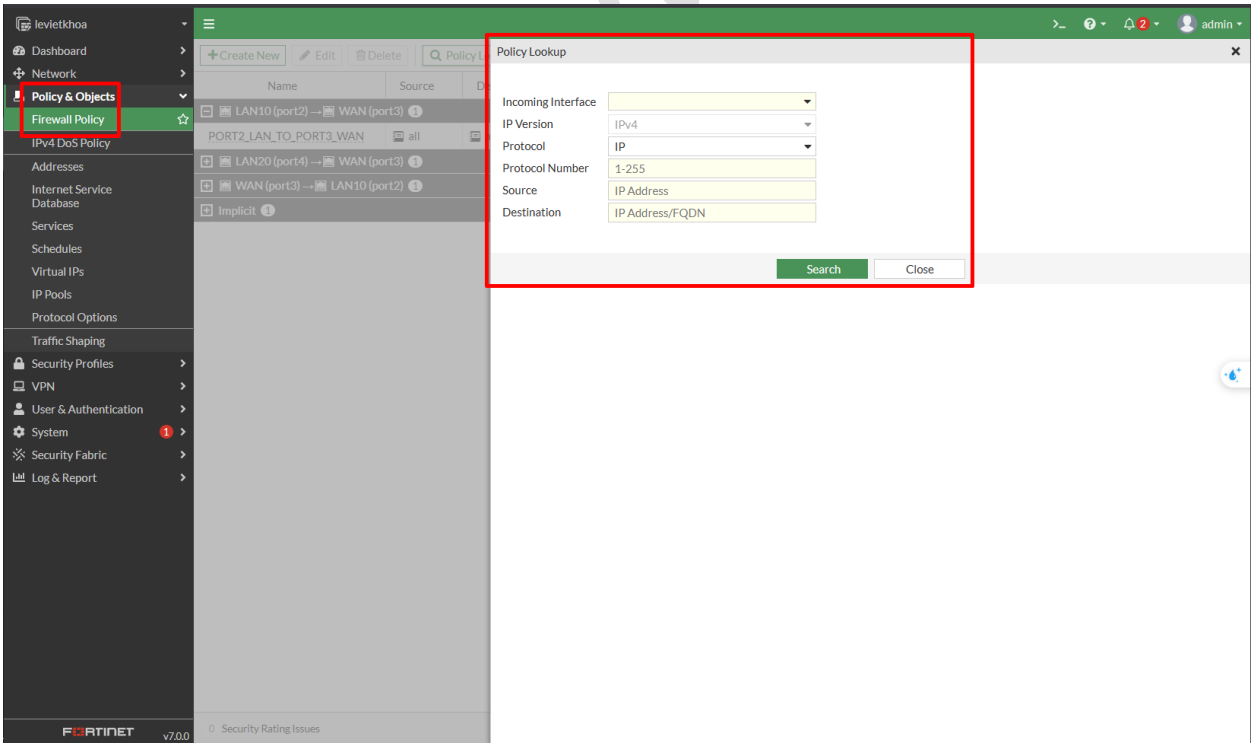
Khi phát sinh sự cố, chúng ta nên tận dụng các công cụ tích hợp sẵn trên FortiGate để chẩn đoán và xử lý kịp thời.

Công cụ hỗ trợ

– Policy Lookup

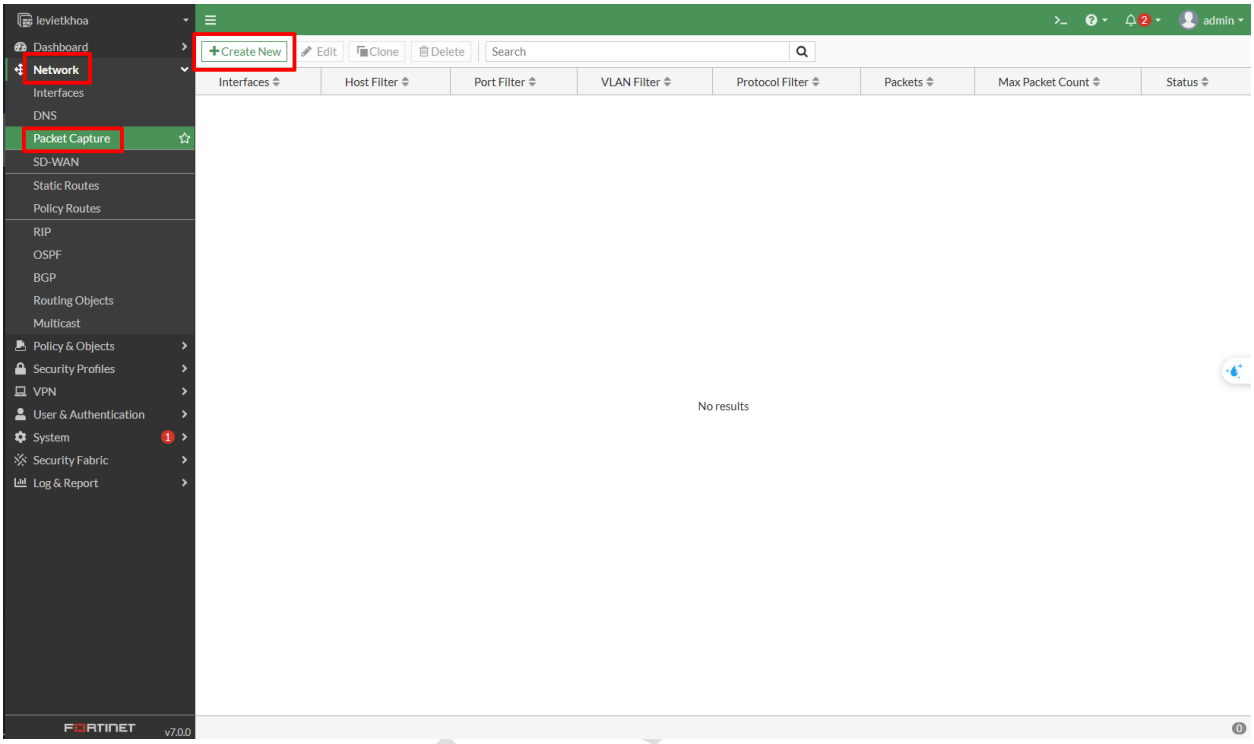
Vào **Policy & Objects > Firewall Policy**, nhập **Source IP**, **Destination IP**, port, protocol để xác định traffic khớp với Firewall Policy nào. Đây là bước đầu giúp xác định nguyên nhân sự cố truy cập.

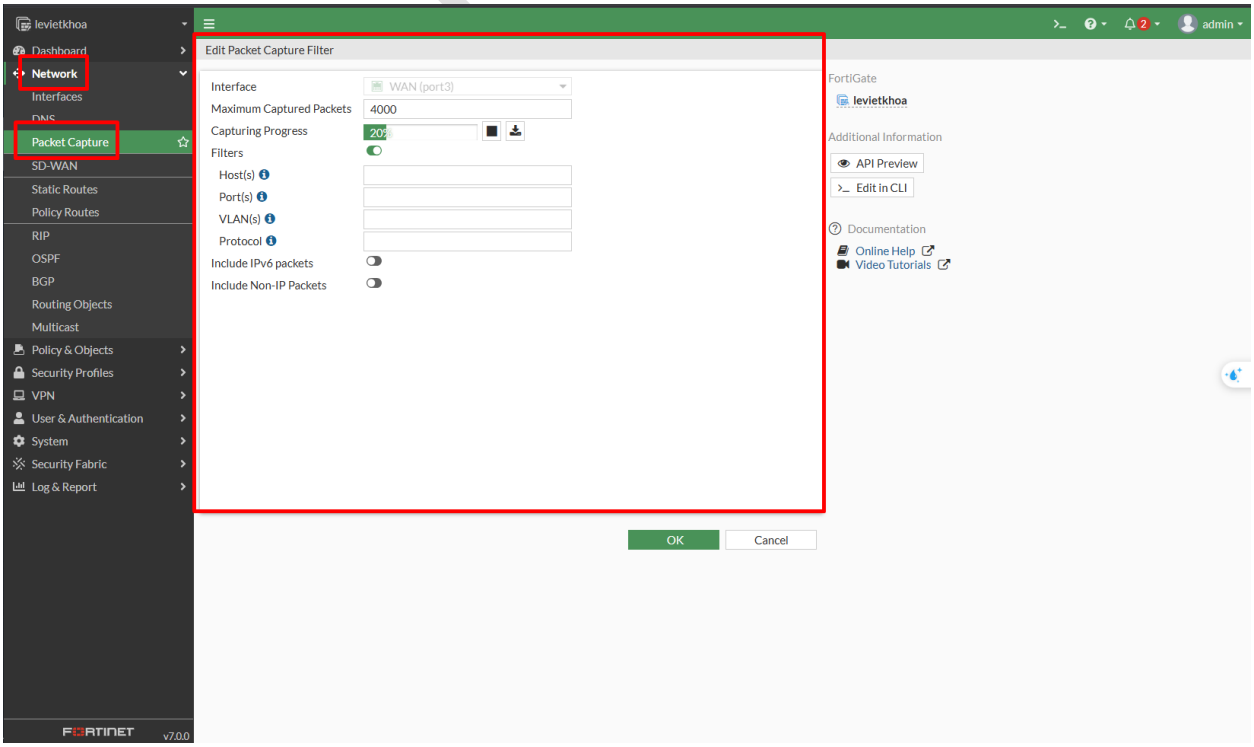

levietkhoa
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
admin
Create New
Edit
Delete
Policy Lookup
Search
Interface Pair View
By Sequence
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
LAN10 (port2) → WAN (port3)
PORT2_LAN_TO_PORT3_WAN
all
all
always
ALL
ACCEPT
Enabled
no-inspection
All
216.48 MB
LAN20 (port4) → WAN (port3)
WAN (port3) → LAN10 (port2)
Implicit
FORTINET
v7.0.0
Security Rating Issues
Updated: 16:30:58


levietkhoa
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
admin
Policy Lookup
Incoming Interface
IP Version
IPv4
Protocol
IP
Protocol Number
1-255
Source
IP Address
Destination
IP Address/FQDN
Search
Close
FORTINET
v7.0.0
Security Rating Issues

– Packet Sniffer

Trên giao diện FortiGate, tính năng Packet Sniffer (Network > Packet Capture) cho phép chọn interface, áp dụng bộ lọc (host, port…) để xem lưu lượng thô theo thời gian thực, hỗ trợ phân tích sâu khi cần thiết.





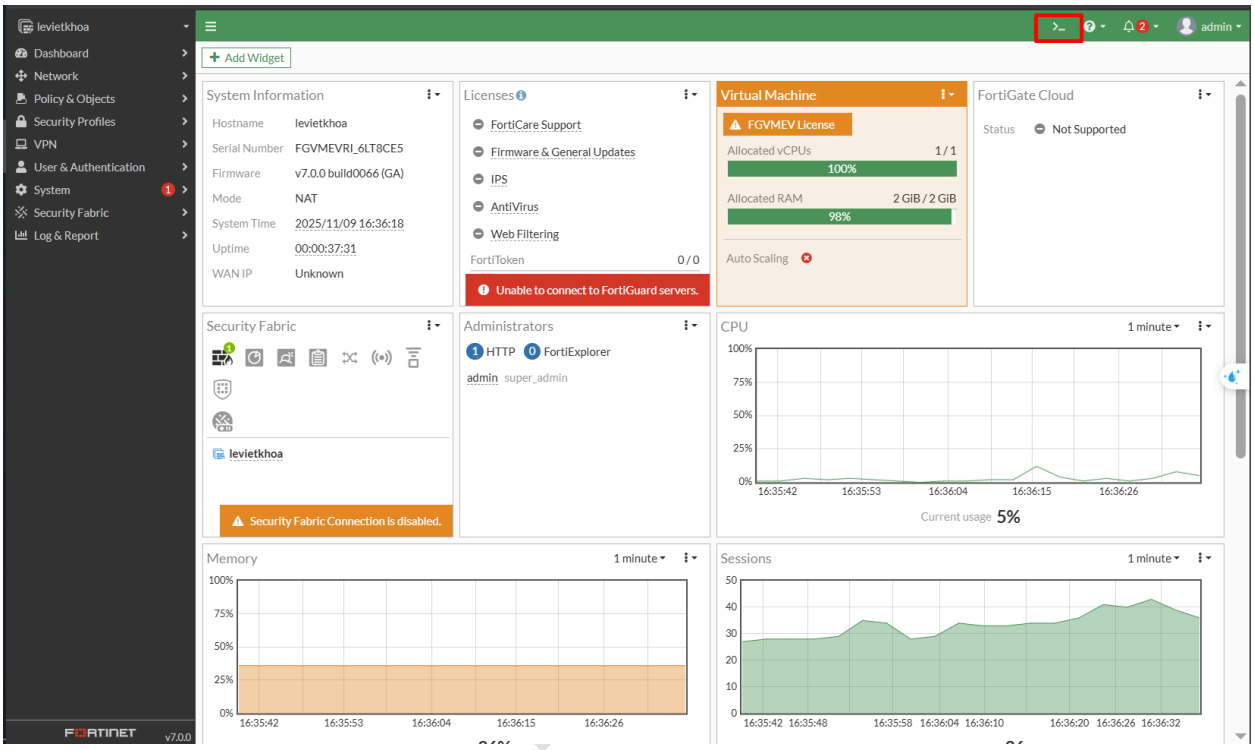
– CLI Diagnostics

Chúng ta sử dụng CLI Console với các lệnh chẩn đoán phổ biến như:

– **diag debug flow**: Hiển thị chi tiết từng bước xử lý gói tin, nên sử dụng kèm bộ lọc để tránh quá tải thông tin.

– **execute ping**: Kiểm tra kết nối cơ bản với đích mong muốn.

– **get system performance status**: Xem nhanh trạng thái CPU và bộ nhớ hệ thống.



Best Practices

– Thiết lập lịch trình sao lưu định kỳ (hàng tuần hoặc hàng tháng) để đảm bảo an toàn cấu hình.

– Đối với hệ thống quản lý nhiều thiết bị FortiGate, nên sử dụng giải pháp logging tập trung như **FortiAnalyzer** hoặc **FortiCloud** để tối ưu hóa công tác quản trị.

– Tài liệu hóa toàn bộ các thay đổi cấu hình quan trọng và giải thích lý do thay đổi để thuận tiện cho việc theo dõi, bàn giao hoặc rà soát sau này.

Mẹo kỹ thuật: Khi xử lý sự cố, chúng ta nên bắt đầu từ Policy Lookup, tiếp theo sử dụng Packet Sniffer và CLI để phân tích sâu hơn, giúp tiết kiệm thời gian và nâng cao hiệu quả chẩn đoán.

8. Phụ lục và Tham khảo

Phần này tổng hợp các nguyên tắc và kinh nghiệm thực tiễn, giúp chúng ta thiết kế hệ thống FortiGate an toàn, dễ quản lý và hạn chế lỗi phát sinh trong quá trình vận hành.

8.1 Best Practices tổng hợp

Các nguyên tắc và kinh nghiệm triển khai dưới đây giúp chúng ta xây dựng hệ thống FortiGate vững chắc, tối ưu hóa quản trị và bảo mật.

1. Nguyên tắc thiết kế Firewall Policy

- – **Đặt tên rõ ràng, nhất quán:** Sử dụng tên policy theo chuẩn Fortinet, ví dụ: *Allow_Marketing_to_Web*, *Deny_Guest_to_Internal*. Cách đặt tên này giúp nhận diện nhanh chức năng và đối tượng áp dụng của từng policy.
- – **Nguyên tắc Least Privilege (Quyền tối thiểu):** Chỉ cấp quyền truy cập thực sự cần thiết cho từng đối tượng. Hạn chế sử dụng 'all' trong Source/Destination/Service nếu không bắt buộc nhằm giảm thiểu rủi ro bảo mật.
- – **Thứ tự policy:**
  - – Policy cụ thể (Specific Policy) cần đặt ở trên cùng.
  - – Policy chung, phạm vi rộng hơn (General Policy) đặt phía dưới.
- – Mỗi policy nên có mô tả ngắn gọn về mục đích sử dụng để hỗ trợ rà soát, bàn giao hoặc kiểm tra lại cấu hình.
- – Khi sử dụng SNAT (Source NAT, truy cập Internet), cần bật NAT trên policy để đảm bảo máy trạm trong LAN có thể truy cập Internet.
- – Khi triển khai DNAT/Port Forwarding (Destination NAT/VIP), tắt NAT trên policy để tránh xung đột và đảm bảo traffic đi đúng đến server nội bộ.

2. Quản lý Object

- – **Đặt tên object rõ ràng:**
  - – Address: *LAN_Network*, *WebServer_Internal_IP* giúp xác định nhanh đối tượng địa chỉ.
  - – Service: *TCP_8080*, *CustomApp_UDP_5000* hỗ trợ quản lý dịch vụ nhất quán.
  - – User Group: *Sales_VPN_Group* thể hiện rõ nhóm người dùng và chức năng.
- – **Chỉ sử dụng 'all' cho Source/Destination khi thực sự cần thiết:** Quy tắc này giúp hạn chế các policy có phạm vi quá rộng, tăng mức độ kiểm soát và bảo mật mạng.

3. Ghi chú mô hình triển khai

- – **VPN:**

    - – **SSL VPN:** Sử dụng cho truy cập từ xa (remote access) dành cho nhân viên; cần kết hợp Firewall Policy và User Group để kiểm soát quyền truy cập.
    - – **IPsec VPN (Site-to-Site):** Áp dụng Wizard, cấu hình Pre-shared Key mạnh, enable Dead Peer Detection (DPD) để tăng độ ổn định kết nối.
- – **DNAT / VIP:** Cho phép truy cập server nội bộ từ Internet (Port Forwarding), cấu hình VIP (Virtual IP) đúng chuẩn, tắt NAT trên policy.
- – **Security Profile:** Gắn các profile như Antivirus, Web Filter, IPS, Application Control, DNS Filter vào các policy phù hợp để nâng cao mức độ bảo vệ hệ thống.

8.2 Các lỗi cấu hình thường gặp

- – **Sai thứ tự policy:** Đặt policy chung lên trên policy cụ thể khiến traffic không được lọc đúng, làm giảm hiệu quả kiểm soát truy cập.
- – **Không bật NAT khi cần SNAT:** LAN không thể truy cập Internet do thiếu cấu hình NAT trên policy.
- – **Bật NAT khi dùng DNAT/VIP:** Traffic không đi đúng server nội bộ, gây lỗi truy cập dịch vụ.
- – **Sử dụng 'all' source/destination quá mức:** Tăng rủi ro bảo mật, khó kiểm soát traffic.
- – **Object trùng hoặc thiếu:** Nhập IP/Port trực tiếp thay vì tạo object dẫn đến khó quản lý, dễ nhầm lẫn và tiềm ẩn lỗi cấu hình.
- – **Bỏ qua backup trước thay đổi:** Nâng cấp firmware hoặc thực hiện thay đổi lớn mà không sao lưu cấu hình dẫn đến nguy cơ mất dữ liệu cấu hình.
- – **Không gắn Security Profile:** Không cấu hình Web Filter, IPS, Antivirus trên policy làm giảm mức độ bảo vệ, tăng nguy cơ bị tấn công.

Tóm tắt

- – **Quản trị chặt chẽ – rõ ràng – có ghi chú:** Giúp hệ thống dễ quản lý, thuận tiện cho kiểm tra và bàn giao.
- – **Luôn sao lưu – kiểm tra policy – gắn Security Profile:** Giảm lỗi, tăng tính bảo mật và khả năng phục hồi hệ thống.
- – **Tên object và policy nhất quán:** Tạo tiền đề thuận lợi cho việc mở rộng, bảo trì dài hạn.